# FORE Systems
# ES-2810 Ethernet Switch
# User's Manual

MANU0330-01 - Rev. A - June, 1998

Firmware Version 2.20

Stack View Version 1.51

FORE Systems, Inc.

1000 FORE Drive

Warrendale, PA 15086-7502

Phone: 724-742-4444

FAX: 724-772-6500

URL: http://www.fore.com

## *Legal Notices*



## *FCC CLASS A NOTICE*

**WARNING**: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void this user's authority to operate this equipment.

NOTE: The ES-2810 Ethernet Switch has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of the equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

## *CE NOTICE*

Marking by the symbol **CE** indicates compliance of this system to the EMC (Electromagnetic Compatibility) directive of the European Community and compliance to the Low Voltage (Safety) Directive. Such marking is indicative that this system meets or exceeds the following technical standards:

- EN 55022 - "Limits and Methods of Measurement of Radio Interference Characteristics of Information Technology Equipment."
- EN 50082-1 - "Electromagnetic compatibility - Generic immunity standard Part 1: Residential, commercial, and light industry."
- IEC 1000-4-2 - "Electromagnetic compatibility for industrial-process measurement and control equipment Part 2: Electrostatic discharge requirements."
- IEC 1000-4-3 - "Electromagnetic compatibility for industrial-process measurement and control equipment Part 3: Radiate electromagnetic field requirements."
- IEC 1000-4-4 - "Electromagnetic compatibility for industrial-process measurement and control equipment Part 4: Electrical fast transient / burst requirements."
- IEC 1000-4-5 - "Electromagnetic compatibility - Generic immunity standard Part 5: Surge test."

## *CERTIFICATIONS*

ETL certified to meet Information Technology Equipment safety standards UL 1950, CSA 22.2 No. 950, and EN 60950.

## *TRADEMARKS*

# Table of Contents

**CHAPTER 2 Introduction to Stack View**

# List of Figures

# Preface



This manual provides the necessary information to install the FORE Systems® ES-2810 Ethernet switch. Also included is general product information, network configuration information and information about software administration capabilities. This manual is for users with various levels of experience.

If you have any questions or problems with the installation, please contact FORE Systems' Technical Support using the information on page ii.

## Chapter Summaries

**Chapter 1 - Introduction to the ES-2810 -** Provides an overview of the ES-2810 switch and installation procedures for the switch and its modules.

**Chapter 2 - Introduction to Stack View -** Provides an overview of the Stack View network management software for the ES-2810.

**Chapter 3 - Standard Configuration -** Provides information on doing a standard configuration of the ES-2810.

**Chapter 4 - Advanced Configuration -** Provides information on doing an advanced configuration using virtual LANs (VLANs).

**Chapter 5 - Managing the Switch -** Provides information on managing the ES-2810 using the Stack View network management software.

**Chapter 6 - Technical Specifications** - Provides physical, power and performance specifications for the ES-2810 and its modules.

**Chapter 7 - Troubleshooting** - Provides a troubleshooting checklist for the ES-2810.

**Appendix A - Concepts in Switching** - Provides a basic overview of switching concepts including forwarding modes, flow control, filtering, IP, etc.

# Technical Support

In the U.S.A., customers can reach FORE Systems' Technical Assistance Center (TAC) using any one of the following methods:

1. Select the "Support" link from FORE's World Wide Web page:

   **http://www.fore.com/**

2. Send questions, via e-mail, to:

   **support@fore.com**

3. Telephone questions to "support" at:

   **800-671-FORE (3673)** or **724-742-6999**

4. FAX questions to "support" at:

   **724-742-7900**

Technical support for customers outside the United States should be handled through the local distributor or via telephone at the following number:

**+1 724-742-6999**

No matter which method is used to reach FORE Support, customers should be ready to provide the following:

- A support contract ID number
- The serial number of each product in question
- All relevant information describing the problem or question

# Typographical Styles

Throughout this manual, all specific commands meant to be entered by the user appear on a separate line in bold typeface. In addition, use of the `Enter` or `Return` key is represented as **<ENTER>**. The following example demonstrates this convention:

```
cd /usr <ENTER>
```

File names that appear within the text of this manual are represented in the following style: "... refer to the `README.TXT` file on the CD..."

Command names and GUI control buttons that appear within the text of this manual are represented in the following style: "Choose the **`Start`** button on the Taskbar."

Parameter names that appear within the text of this manual are represented in the following style: "The **|<***range***>** is an optional part...."

Any messages that appear on the screen during software installation and network interface administration are shown in `Courier` font to distinguish them from the rest of the text as follows:

```
.... Are all four conditions true?
```

# Important Information Indicators

To call your attention to safety and otherwise important information that must be reviewed to insure correct and complete installation, as well as to avoid damage to the FORE adapter or your system, FORE Systems utilizes the following *WARNING/CAUTION/NOTE* indicators.

*WARNING* statements contain information that is critical to the safety of the operator and/or the system. Do not proceed beyond a *WARNING* statement until the indicated conditions are fully understood or met. This information could prevent serious injury to the operator and damage to the FORE adapter, the system, or currently loaded software, and will be indicated as:

***WARNING!***

Hazardous voltages are present. To lessen the risk of electrical shock and danger to personal health, follow the instructions carefully.

Information contained in CAUTION statements is important for proper installation/operation. Compliance with CAUTION statements can prevent possible equipment damage and/or loss of data and will be indicated as:

**CAUTION**

You risk damaging your equipment and/or software if you do not follow these instructions.

Information contained in NOTE statements has been found important enough to be called to the special attention of the operator and will be set off from the text as follows:


Steps 1, 3, and 5 are similar to the installation for the computer type above. Review the previous installation procedure before installation in your particular model**.**

# Safety Agency Compliance

This preface provides safety precautions to follow when installing a FORE Systems, Inc., product.

## Safety Precautions

For your protection, observe the following safety precaution when setting up your equipment:

- Follow all warnings and instructions marked on the equipment.
- Opening this product must only be done by a network manager or person who is qualified and authorized to install electrical equipment, and who is aware of the hazards to which he/she is exposed. This person must have an advanced technical background within data communications and networks.

## Symbols

The following symbols appear in this book.

**CAUTION**

If instructions are not followed, there is a risk of damage to the equipment.

***WARNING!***

Hazardous voltages are present. If the instructions are not heeded, there is a risk of electrical shock and danger to personal health.

## Modifications to Equipment

Do not make mechanical or electrical modifications to the equipment. FORE Systems, Inc., is not responsible for regulatory compliance of a modified FORE product.

# CHAPTER 1 Introduction to the ES-2810

This chapter covers the topics listed in Table 1.1.

**Table 1.1 -** Topics in this Chapter

| For Information on This Topic... | Refer to... |
|---|---|
| Introduction to the product | page 1-2 |
| Front Panel | page 1-4 |
| Rear Panel | page 1-6 |
| Installation | page 1-8 |
| Restoring the Software | page 1-22 |
| Recovering from Start-up Failure | page 1-24 |

# 1.1 Introduction to the Product

## 1.1.1 Purpose of the Switch

This Ethernet switch uses your existing network cables to integrate switching technology into your computer network.

With the switch, each device in a workgroup or a network segment can communicate at a full wire-speed of 10 Mbps or 100Mbps to provide:

- High-speed connectivity
- Simultaneous two-way communication between connected devices
- Increased network throughput and performance
- Increased server availability

## 1.1.2 Physical Features

This switch offers the following features:

- Plug-and-play—no need to configure the module to use the basic operations
- Provides 24 x 10 / 100 Mbps connections
- Two option slots for Media Modules
- Front panel LEDs show switch, port and traffic status
- Automatic detection of 100 V and 240 V power supplies

## 1.1.3 Hardware Features

The switch offers the following features:

- Each port operates in a choice of switching modes: cut-through, fragment-free or store-and-forward
- Each port supports half- and full-duplex operation
- Simultaneous full wire speed switching on all ports
- RMON support for Statistics, History, Alarm and Events
- Spanning Tree support on all ports
- Flow control
- Permanent MAC address entries

### 1.1.4 Software Features

The switch offers the following features:

- Stack View for Windows* 95 and Windows NT*
- Adaptive forwarding mode
- Local Management via a direct terminal connection or via TELNET
- SNMP Management support
- BOOTP and TFTP support
- Control over user access rights
- Creation of virtual LANs

# 1.2 Front Panel

## 1.2.1 Introduction

The LEDs on the front panel shows the state of the ports, so you should position the switch with the front panel facing you. You can also see which ports the cables are connected to on the switch.

## 1.2.2 View of the Front Panel

The front panel of the switch is shown below:

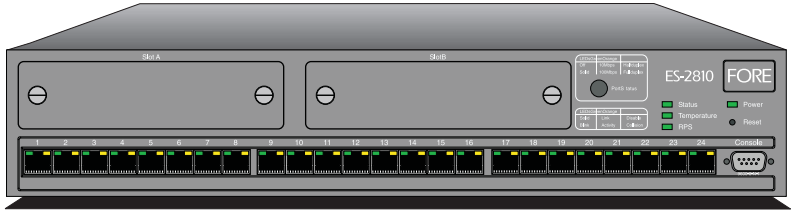



**Figure 1.1 -** ES-2810 Front Panel

## 1.2.3 Front panel ports

The following ports are on the front panel:

**Table 1.2 -** Front Panel Ports

| Port | Function |
|---|---|
| CONSOLE port (DB-9) | Connects a PC (running a VT100 emulation), a VT100 terminal or a modem to access the in-built Local Management program. |
| 24x 10/100Base-TX ports (RJ-45) | To connect devices using Unshielded Twisted Pair (UTP) cabling complying to EIA 568A Category 5 or ISO/IEC 11801 Category 5 level D. |

## 1.2.4 Slots for Media Modules

After removing one or both of the covers, the following Media Modules can be inserted in the front of the switch:

**Table 1.3 -** ES-2810 Media Modules

| Product Name | Function |
|---|---|
| 10/100TX Module | Adds 4 x 10/100Base-TX ports (RJ-45) |
| 100FX Module | Adds 2 x 100Base-FX ports (SC) |



## 1.2.5 Front Panel LED Functions

The LEDs on the front panel have the following functions:

**Table 1.4 -** Front Panel LEDs

| LEDs | Function |
|---|---|
| Green and Yellow | Indicates the operational status of each port. |
| Status | Gives the operational status of the switch. |
| Power | Show the status of the internal power supply. |
| Temperature | Show the status of the internal temperature. |
| RPS (redundant power supply) | Show the status of the external, redundant power supply. |

## 1.2.6 Buttons

The buttons on the front panel have the following functions:

**Table 1.5 -** Front Panel Buttons

| Button name | Function |
|---|---|
| Port Status | To show the operational status of each port. |
| Reset | Reset or enter Maintenance Mode |

# 1.3 Rear Panel

## 1.3.1 Introduction

The rear panel has a cooling fan outlet and the main supply cable, so you should position the switch with the rear panel facing away from you.

## 1.3.2 View of Rear Panel

The rear panel of the switch is shown below:

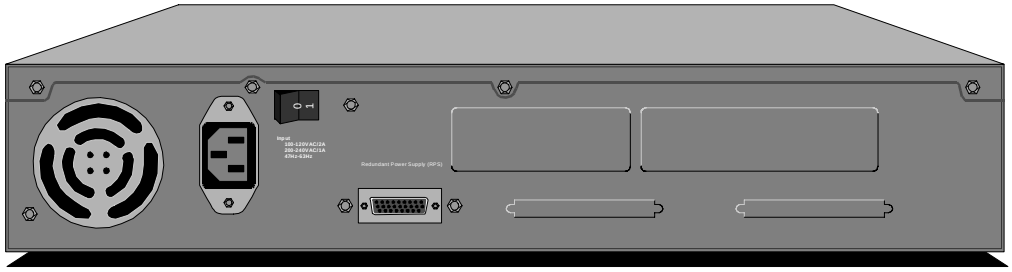


**Figure 1.2 -** ES-2810 Rear Panel

### 1.3.3 Rear Panel Parts

The rear panel of the switch has the following parts:

**Table 1.6 -** Rear Panel Parts

| Part | Function |
|---|---|
| Fan outlet | To cool the internal circuitry of the switch |
| Power connection | A socket to connect the power cord to the main supply. |
| Mains control (ON / OFF) | To provide power from the main supply. |
| Redundant power supply connector | To connect an external redundant power supply. If the internal power supply fails, the redundant power supply starts immediately. |

# 1.4 Installation

## 1.4.1 Important

All local and national regulations governing the installation and connection of electrical devices must be strictly adhered to when installing the switch.

# 1.5 Before Installation

## 1.5.1 Contents of the Pack

Unpack the switch carefully and check that all parts are present, as described in the packing list.

## 1.5.2 Check the Package Contents

If you have not received all of the parts, or any of the parts are damaged, contact your dealer immediately.

Keep all the packaging materials in case you need to repack the switch.

## 1.5.3 Check All Labels

Read all labels and rating plates on the switch. If there is anything that you do not understand, or if any of the information provided does not appear to comply with your local or national rules and regulations, consult your dealer before proceeding with the installation.

## 1.5.4 Essential Reading

It is important that you read the following:

- ES-2810 Release Notes

  This contains information you should be aware of when installing and using the product, for example, limitations and compatibility issues.
- Warnings and the instructions earlier in this guide.
- The `README.TXT` file on the Compact Disk. This gives a general description of the software and specific requirements.

# 1.6 Positioning the Switch

## 1.6.1 Allow Adequate Ventilation

The switch contains two fans to air-cool the internal circuitry. The air is drawn in from the left of the unit and expelled through the outlet grills on the right side and the rear.

To ensure correct airflow, leave 100 mm (4 inches) free space on both the sides and back of the of the switch. Do not allow the inlet or outlet grills to become blocked.



## 1.6.2 On a Desktop

To install the switch in a desktop environment:

1. Find the four rubber feet in the pack that contains the rack mounting kit.
2. Remove the backing strip from each of the four feet.
3. Attach the four rubber feet to the underneath of the switch (to ensure that the switch stands firmly).
4. Place the switch on a stable, flat surface.
5. Ensure that the air intake (on the left) and fan outlets (on the right side and rear) are not blocked.

***WARNING!***

The switch's lifetime and operational reliability can be seriously degraded by inadequate cooling.

## 1.6.3 Rack Requirements

The switch should be installed in a standard rack in accordance with IEC 297 (or similar); if the minimum outside measurements of the rack are 600 x 600 mm (23.5 x 23.5 inches), you must allow 190 mm (7.5 inches) of space at the rear.

## 1.6.4 Mounting kit

The switch is delivered with a kit to attach it to a standard 19-inch equipment rack (with side support rails). The kit contains two mounting brackets and four screws (for attaching the brackets to the sides of the switch).

***WARNING!***

The switch must only be installed in an equipment rack which has side support rails. The mounting brackets are used only to secure the switch in the rack and must not support its weight.

## 1.6.5 Tools Required for Positioning in a Rack

You need the following items for mounting the switch in a rack:

- Standard 19-inch rack with side support rails
- A rack mounting kit (included)
- 3 mm screwdriver
- Customer-supplied screws for securing the switch in the rack

  Mounting screws are not provided because the required sizes may vary from rack to rack.

## 1.6.6 In an Equipment Rack

To mount the switch in a standard equipment rack, proceed as follows:

1. Attach the mounting bracket marked “Left” to the left-hand side of the switch, and attach the mounting bracket marked “Right” to the right-hand side of the switch, using the four screws provided.

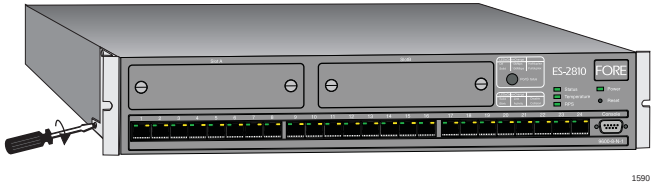



**Figure 1.3 -** Attaching the Mounting Brackets

   It is important to attach the mounting brackets to the correct sides. Otherwise the switch will not be aligned correctly in the equipment rack.

2. If the four rubber feet prevent the switch from standing firmly on the equipment rack’s side support rails, remove the feet.

3. Set the switch in the equipment rack and ensure there is adequate ventilation (see "Allow Adequate Ventilation" on page 1-9).
4. Screw the mounting brackets securely to the equipment rack.

## 1.6.7 Ambient Temperature

If the switch is installed in a closed or multi-rack assembly, the operating ambient temperature of the rack environment may be greater than the ambient temperature of the room. Care must be taken to ensure the temperature of the rack environment does not exceed the recommended operating temperature for the switch.

# 1.7 Installing a Media Module

You can increase the connectivity options of your switch by installing a media module.

***WARNING!***

Media modules are not designed to be installed in, or removed from, the switch while it is in operation. You must power off the switch before attempting to install a media module.

## 1.7.1 Static-free Working Area

The printed circuit board is an Electrostatic Sensitive Device and should not be handled except at a static-free working area, otherwise the printed circuit board may fail or be degraded.

## 1.7.2 Avoiding Damage to the Circuit Board

If you open the switch, for example, to install a media module, follow this procedure to avoid damage to your printed circuit board:

***WARNING!***

The switch must not be opened unless it has been disconnected from the main power supply.

1. Ensure that the switch is disconnected from the main power supply.
2. Make sure that the switch is grounded before you handle the printed circuit board.
3. Connect yourself to a non-painted / non-isolated part of the grounded switch (for example the back panel) by means of a wrist strap with 1MΩ resistance to ensure that you carry the same electrostatic charge as the enclosure.
4. Now you can open the switch.

## 1.7.3 To Install a Media Module

To install a media module, proceed as follows:

1. If the switch is already operational, disconnect it from the main power supply.

2. Remove the screws of the blank panel covering the media module port at the rear of the switch. Save these screws and plate.
3. Look inside to see the position of the media module guide-rails inside the switch.
4. Position the corners of the circuit board in the entrance to the guide-rails and carefully push the media module in. Ensure that the media module connectors engage fully with the socket on the motherboard.
5. Secure the media module in place using the screws provided.

## 1.7.4 To Remove the Media Module

To remove a media module:

1. Remove the screws securing the media module.
2. Pull the media module gently to disengage the connectors fully from the socket on the motherboard. Slide the media module out completely.
3. Cover the empty media module port with the blank panel and secure using the screws.

# 1.8 Connecting Other Devices

Incorrect cabling is often the cause of network configuration problems.

## 1.8.1 Use Shielded Cables

Shielded cables normally comply with EMC and FCC emission limits.

Only use unshielded cables when it is explicitly specified in the installation manual of the device in question.

## 1.8.2 Cables for the LAN Ports

Ports on the switch are wired MDI-X, so use the following cable:

**Table 1.7 -** LAN Port Cable Usage

| If you connect the switch to a | Then use a |
|---|---|
| Workstation or server | Straight-through cable 1:1 |
| Device with MDI-X ports (for example another FORE Systems switch or hub) | Crossover cable |
| Device with MDI ports | Straight-through cable 1:1 |

## 1.8.3 RJ-45 Connector Pin Assignments

The 24 RJ-45 ports on the front of the switch have the following pin assignments:

**Table 1.8 -** RJ-45 Pin Assignments

| Pin number | Function |
|---|---|
| 1 | RX+ |
| 2 | RX- |
| 3 | TX+ |
| 6 | TX- |

## 1.8.4 Cable for the Console Port

If you connect a PC (via the Console Port), then use a null-modem cable.

## 1.8.5 To Connect a Device to the RJ-45 Ports

To connect a workstation compatible with IEEE 802.3 (Ethernet Version 1.0 and 2.0) or a fast access device (such as a server) to the switch's RJ-45 ports using UTP cable (Category 5):

1. Ensure that the device has a 100Mbps (100Base-FX or 10/100Base-TX) network interface card installed.

   If not, use your network interface card's documentation to install and configure it correctly.

2. If your workstation is fitted with an RJ-45 interface then there is no problem. However, it is possible to attach to other connector types using an appropriate adapter. For example, use a UTP/10Base-FL adapter for fiber connections

3. Connect one end of the UTP cable to an RJ-45 port on the switch.

   According to IEEE 802.3, the cable length must not exceed 100 meters (approximately 325 feet).

4. Connect the other end to the 100Base-TX connection on the device.

# 1.9 Connecting the Power

After connecting the devices to the switch, connect the power cable. There are certain practical and safety considerations to be made before powering the switch on.

## 1.9.1 The Power Cable

### 1.9.1.1 Ground Warning

The switch is delivered with a power cable to fit the power sockets in your country. If this is not the case, contact your dealer immediately and ask for the correct power cable.

### 1.9.1.2 Power Cable Wiring Color Code

The wires in the power cable provided with this equipment are colored in accordance with the following code:

**Table 1.9 -** Wiring Color Codes

| Color | Connection |
|---|---|
| Green and yellow | Ground |
| Blue | Neutral |
| Brown | Live |

### 1.9.1.3 Important for UK Use

The colors of the wires in the power cable provided with this equipment may not correspond with the markings which identify the terminals in your plug, use the following procedure:

1. Check that the wire colored green and yellow is connected to the terminal which is marked with the letter E, or by the ground symbol ⏚ or colored green and yellow.
2. Check that the wire colored blue is connected to the terminal which is marked with the letter N or colored black.
3. Check that the wire colored brown is connected to the terminal which is marked with the letter L or colored red.

#### 1.9.1.4 Power Supply to a Rack

If the switch is installed in a rack, ensure the rack's power supply socket has a ground connection and the rack is connected to a branch supply or a power supply socket with a ground connection.

To avoid overloading the circuit and damaging the wiring of the power supply, ensure the power supply to the rack is adequate to cover the extra power consumed by the switch.

#### 1.9.1.5 Lithium Battery

This equipment contains a component (DS1603) with a lithium battery. Dispose of the switch like a lithium battery.



### 1.9.2 Power-up

#### 1.9.2.1 Powering-up the Switch

Follow the steps to power-up the switch:

1. Press the mains switch (on the rear panel) to off.
2. Push the female end of the power cable into the mains socket (in the rear panel), and plug the other end into the power supply outlet.
3. Press the mains switch (on the rear panel) to on.
4. Check that the Power LED (on the front panel) becomes green.

   If it is not green, check that the power outlet is working correctly (switched on). If the power outlet is on and the Power LED is not green, then there is a fault within the switch and you must contact your dealer.
5. Verify that a LED is lit for each of the front panel ports to which a powered-on device is connected.

### 1.9.2.2 Start-up Procedure

Immediately after power-up, the following should happen during start-up:

**Table 1.10 -** Start-up Procedure

| Stage | When the STATUS LED... | Then the Switch... |
|---|---|---|
| 1 | Is red | Is starting up |
| 2 | Turns to steady green | Has started successfully |
| 3 | Remains red | Has not started successfully. Try to restart it. If the switch has still not started, contact your dealer |

Look at the other front panel LEDs during start-up and check that they are operating correctly.

### 1.9.2.3 Port LED States

The LEDs reflect the state of each port:

**Table 1.11 -** Port LED States

| Green | Yellow | Shows |
|---|---|---|
| Off | Off | Port enabled, no link. |
| Blinking randomly | Off | Port enabled, Rx / Tx traffic, link pulse active. |
| Solid | Off | Port enabled, link pulse active. |
| Solid | Blinking randomly | Collision detected.<br>Port enabled, link pulse active. |
| Off | Solid | Port disabled by hardware failure or management. |
| Solid | Solid | Port disabled by a fault, or no hardware connected. |
| Off | One blink / second | Port has wrong link partner. |

## 1.9.3 Default Settings After Start-up

Once the switch has started successfully, installation is complete and the switch is using its default setting (also known as default configuration):

- All ports are enabled.
- All ports operate in auto-negotiation mode.
- Spanning Tree is disabled on all ports.
- Addresses which have been silent for more than 15 minutes are purged from the switch's address table (the MAC Address Ageing time).
- No access restrictions to Local Management.
- No SNMP restrictions.
- No permanent MAC address entries defined. A permanent entry is a MAC address which is defined as being permitted only on a certain port, and can be a useful security feature.
- All ports, IP addresses and MAC addresses are in the same VLAN (named <System>). VLANs allow you to create virtual networks using specific switch ports, IP addresses and MAC addresses.
- Local Management time-out after 10 minutes.

### 1.9.3.1 After Start-up

This default configuration is adequate for simple workgroup environments to operate in basic switching mode.

Although the switch continues to operate without problems, we recommend that you change certain parameters to suit your own requirements.

Follow the instructions in chapter 2 to change the configuration while the switch is operating.

# 1.10 Other LEDs on the Front Panel

## 1.10.1 Introduction

There are three other LEDs and one button (on the front panel) to show how the switch is operating:

- Status LED
- Temperature LED
- Redundant Power Supply (RPS) LED
- Port Settings button

## 1.10.2 LED Colors and Their Meanings

The LEDs give information about the state of the switch:

**Table 1.12 -** LED Colors

| LED | Color | Meaning |
|---|---|---|
| Status | Green | Solid: The switch is operating normally. |
| | | Blinking (1 Hz): Updating software or forced boot. |
| | | Blinking (5 Hz): Running in maintenance mode. |
| | Red | Resetting the switch, detecting hardware errors or software traps. |
| Temperature | Green | Normal operating temperature. |
| | Orange | Temperature is higher than normal. Check the area around the air intakes and vents are clear of obstructions. |
| | Red | Temperature is too high and the switch will shut down |
| RPS | Green | Off: No RPS connected. |
| | | Solid: RPS connected, but not needed. |
| | Red | Normal power supply has failed and the RPS has taken over. |

## 1.10.3 Port Status Button

To see the actual speed and duplexity of all the ports, press the **Port Status** button. The LEDs on the ports have a different meaning for 5 seconds.

**Table 1.13 -** Port Status LED Colors

| LED | Color | Meaning |
|---|---|---|
| Left (Speed) | Green | Off: 10Mbps |
| | | Solid: 100 Mbps |
| Right (Duplex) | Orange | Off: Half duplex |
| | | Solid: Full duplex |

# 1.11 Restoring the Software

The switch has all the software (including a default configuration) in its memory (Flash Memory). You can copy this software to a TFTP client using TFTP. If the software in the switch's Flash Memory is corrupted, you can restore the software in the switch using the backup copy.

## 1.11.1 Files Suitable for TFTP Transfer

You can restore the switch's software and retrieve log files for analysis using TFTP. There are various files suitable for TFTP transfer:

**Table 1.14 -** TFTP Suitable Files

| Type | Name | Contains |
|---|---|---|
| ASCII | `report` | Information for FORE Systems Technical Assistance Center (TAC). |
| | `log` | List of errors |
| Binary | `miaram` | Information for FORE Systems TAC. |
| | `filter` | |
| | `inxxxxx.p` | For example `in9eb003.p`. A read/write parameter file which contains the information for configuring a switch somewhere else on the network. |
| | `inxxxxx.nvp` | VLAN database |

## 1.11.2 Transferring files to and from the switch using TFTP

To transfer files using TFTP, proceed as follows:

1. At the command prompt on the Windows, Unix*, or included application, type **tftp <***target switch IP address***>** to start a TFTP session with the switch.
2. Type **get dir** to obtain a directory listing of all the files on the switch.
3. Examine the directory listing to confirm the names of the files present in the switch.

   Report, log and filter files and a parameter file with the extension `.p` or `.nvp` appear in the directory listing.
4. Type **get <***filename***>** to retrieve the file that you want.


If you "get" a report, then the report file is generated on-the-fly and transferred.

5. If the TFTP access is password protected, then type **get<***password***>/<***file-name***>**. For example, **get edinburgh/report**.

# 1.12 Recovering from Start-up Failure

## 1.12.1 Network Boot Process

The network boot process is as follows:

1. The switch sends a BOOTP request over the network.

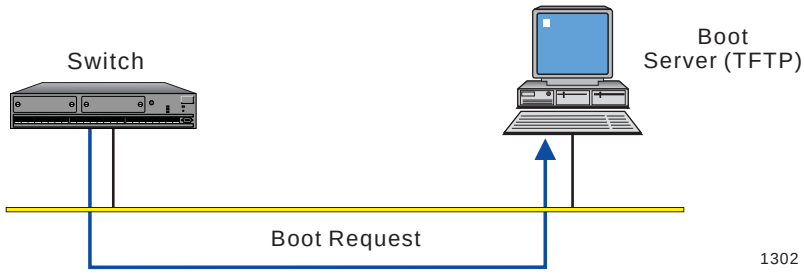



**Figure 1.4 -** Boot Request Process

The boot request contains the switch's MAC address. The boot server contains a bootptab file with an entry for the switch which is defined by the MAC address.

2. If a boot server which holds the software for the switch receives the boot request, it loads the boot software over the network to the destination MAC address.

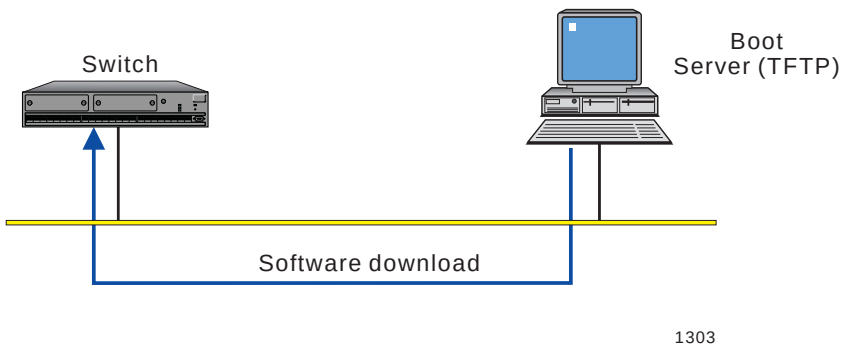



**Figure 1.5 -** Software Download Process

# 1.13 Using Maintenance Mode

## 1.13.1 Purpose

Maintenance Mode offers three facilities:

- It allows you to force the switch to load a specified software file from any specified TFTP server.
- It provides an emergency facility to force boot the switch from a specified boot server if the switch cannot boot from Flash Memory. From Maintenance Mode the switch is forced to issue a BOOTP request and the name of the boot software to a specified boot server. This can be useful in cases where the boot server being used does not support the use of a bootptab file.
- It runs tests on hardware and provides this diagnostic information.




Loading software to the switch in Maintenance Mode should only be done as a last resort, the reason being that the software and configuration already resident in the Flash Memory is overwritten and lost.

## 1.13.2 Important Considerations

There are certain points which need to be considered when using Maintenance Mode:

- In Maintenance Mode, the switch is not operational and the expansion board ports cannot be used.
- Only simple command-line access is possible via the Console port.
- There will be a delay before the command prompt is seen; this is due to a hardware test routine being completed.

## 1.13.3 To Enter Maintenance Mode

To enter Maintenance Mode:

1. Press the **Reset** button on the front of the switch (using a pointed tool — such as a bent paper clip) and hold it until the SYSTEM LED flashes green quickly (5 times per second).
2. Release the **Reset** button.
3. Attach a VT100-compatible terminal to the serial port on the front panel using a serial cable.
4. Press the **<Enter>** key a couple of times until the command prompt appears on the screen of the terminal.

## 1.13.4 Commands Allowed in Maintenance Mode

The following commands are available for the switch in Maintenance Mode.

**Table 1.15 -** Maintenance Mode Commands

| Command | Use |
|---|---|
| **TFTP <***filename***>** *ownIP tftpIP* **[***gwIP***]** | |
| | To load software using the TFTP protocol |
| | <*filename*>: the name of the file containing the software |
| | *ownIP*: your own IP address |
| | *tftpIP*: the IP address of the TFTP host |
| | *[gwIP:* the IP address of the primary router (intermediate gateway)— required if the TFTP server is located on a remote part of the network |
| **BOOTP <***filename***>** | |
| | To load software using the BOOTP or TFTP protocol |
| | <filename>: the name of the file containing the software |
| **DUMP** *addr* | Dump memory contents |
| **INFO** | Show hardware information |
| **RESET** | Resets the switch |
| **RUN** *defparm* | Starts the software in it's default factory settings |

## 1.13.5 Bootptab File Entry

The entry for the switch in the `bootptab` should contain a line similar to:

```
:bf=/fore/switch/es2810_x.xx:
```

This will instruct the switch to load the switch software from the bootp/tftp server. You should use the Stack View application to configure the switch manually, or transfer the `inxxxxxx.p` file containing the configuration from a TFTP server to the switch.

# CHAPTER 2 Introduction to Stack View

This chapter covers the topics listed in Table 2.1.

**Table 2.1 -** Topics in this Chapter

| For Information on This Topic... | Refer to... |
|---|---|
| Installation and Uninstallation | page 2-2 |
| Using FORE Systems Stack View | page 2-5 |
| Stack View (Main Display) | page 2-8 |
| Explorer | page 2-16 |
| Trap Window | page 2-17 |
| System Window | page 2-17 |
| Errors Window | page 2-18 |

# 2.1 Installation and Uninstallation

## 2.1.1 Requirements

The requirements for running FORE Systems Stack View for Windows are:

- A PC with a network adapter installed
- Microsoft Windows NT workstation or server, version 4.0 or 3.51, or Microsoft Windows 95. A Windows NT 4.0 (English language version) workstation is recommended.
- The Microsoft TCP/IP protocol must be installed and configured before installation of FORE Systems Stack View.

## 2.1.2 DHCP Limitation

Two important things to know:

1. Do not use a PC running Windows NT server (with its DHCP server installed) to run Stack View, and
2. Ensure the IP address for the PC is not changed by the DHCP server.

## 2.1.3 Installation Under LANDesk® Network Manager

### 2.1.3.1 LANDesk Network Manager on the PC

If the installation program detects the presence of LANDesk Network Manager on the PC, then Stack View may be integrated under it. After this, double-clicking the icon for a FORE Systems ES-2810 opens Stack View.

### 2.1.3.2 Compilation of MIBS

The order in which the MIBs are compiled is important. The order is:

1. All RFC-MIBS (MIBS with numbers, for example, int_1493.mib) are compiled in increasing numerical order.
2. all other int_????.mibs.

## 2.1.4 Installation Under Windows NT 4.0 and Windows 95

### 2.1.4.1 To Install FORE Systems Stack View

To install FORE Systems Stack View from the CD ROM under Windows NT 4.0 or Windows 95, use Add/Remove Programs from the Control Panel of Windows 95/NT and follow the instructions given on screen.

- Select Typical to install the common features.
- Select Custom to install only selected features.
- Select Compact to install the minimum installation required.

After installation, reboot your PC to make changes to your system files operational.

### 2.1.4.2 Stack View Menu Items

Following successful installation of Stack View for Windows:

- A Stack View (ES-2810 Switch) menu item is added to the Stack View submenu
- An Uninstall Stack View Switch menu item is added under Control Panel>Add/Remove Programs



## 2.1.5 Installation Under Windows NT 3.51

### 2.1.5.1 To Install FORE Systems Stack View

To install FORE Systems Stack View from the CD-ROM under Windows NT 3.51, select Run from the File menu of the Program Manager. Select the Setup program on the CD ROM and select the OK button to start the installation. Follow the instructions given on screen.

- Select Typical to install the common features.
- Select Custom to install only selected features.
- Select Compact to install the minimum installation required.

After installation, reboot your PC to make changes to your system files operational.

## 2.1.6 Program Icons

Following successful installation of FORE Systems Stack View for Windows, two program icons are added to the FORE Systems Stack View program group:

- A FORE Systems Stack View Switch icon
- An Uninstall FORE Systems Stack View Switch icon

# 2.2 Uninstallation of Stack View for Windows

## 2.2.1 Uninstall Under Windows NT 4.0 or Windows 95

To uninstall FORE Systems Stack View under Windows NT 4.0 or Windows 95, proceed as follows:

1. Make sure that you have exited from all FORE Systems Stack View programs.
2. From within the Windows Control Panel, open Add/Remove Programs.
3. Select the FORE Systems Stack View Switch in the list box.
4. Click the **Add/Remove...** button.

## 2.2.2 Uninstall Under Windows NT 3.51

To uninstall FORE Systems Stack View under Windows NT 3.51, proceed as follows:

1. Make sure that you have stopped all FORE Systems Stack View programs.
2. Select the Uninstall Stack View Switch icon from the FORE Systems Stack View folder.

# 2.3 Using Stack View

## 2.3.1 Concept

Stack View is used to configure all the parameters on your switch (via SNMP) and monitor switch activity. The tool used for this purpose is called the Switch Manager, shown in Figure 2.1.

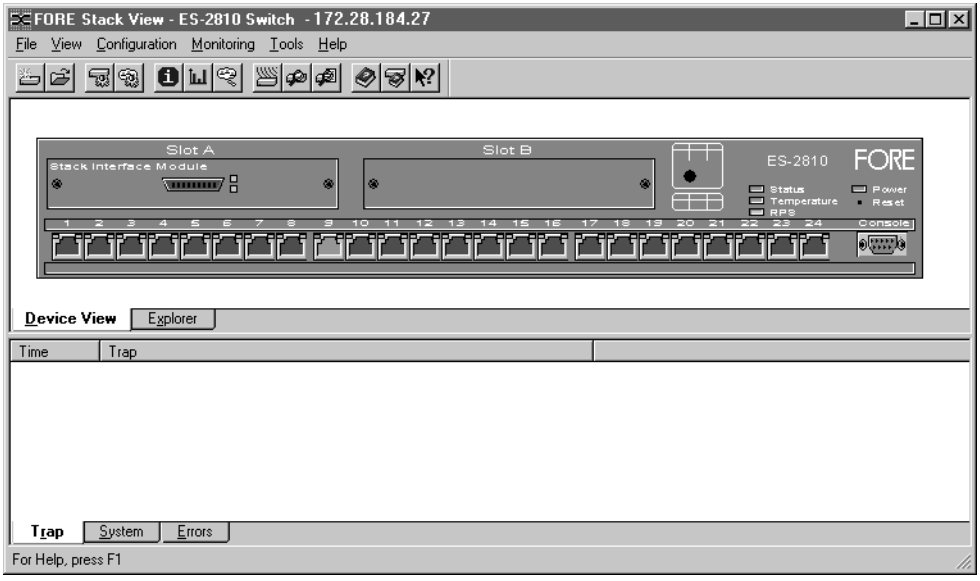



**Figure 2.1 -** Stack View ES-2810 Switch Manager

The Switch Manager displays an interactive picture of the switch showing the port state. From this display, you can show activity statistics for the switch and individual ports.

### 2.3.2 Facilities

Stack View contains the following facilities:

- Switch Manager

  Displays an interactive picture of the switch, receives traps from the switch, and includes extensive SNMP-based monitoring and configuration facilities

- RMON Manager

  Provides distributed network monitoring and alarm facilities

- Report Manager

  Enables TFTP downloading of reports, logs, and traces

- Local Management access

  Provides advanced Telnet access to monitoring functions embedded in the switch

### 2.3.3 Following Installation of FORE Systems Stack View

After installing FORE Systems Stack View, restarting your PC and selecting new, FORE Systems Stack View automatically runs the Install Wizard for you to install your switch.

### 2.3.4 Managing the Switch

To manage a switch which has been assigned an IP address:

1. Click the File>Open menu option.
2. Type the IP address of the switch.
3. Click the checkbox in the File>Open window.

   This will allow you to manage the switch in a new FORE Systems Stack View window.
4. Click the OK button.

### 2.3.5 Adding New Switches

To add additional new switches (which have not been assigned an IP address) to FORE Systems Stack View, select the New Device icon (or select File>New). The Install Wizard will guide you through the installation.

## 2.3.6 The Install Wizard

The Install Wizard requires that you enter the minimum amount of information to set up the switch for management by FORE Systems Stack View.


**Figure 2.2 -** Stack View Install Wizard

The information required includes the MAC address of the switch.

**NOTE** You may need to wait for a few minutes for the switch's MAC address to appear in the list.

You can find the MAC address of the switch on a label on the rear panel.

You will also need to assign an IP address (and subnet mask) to the switch on your Local Area Network (LAN). This address is used by FORE Systems Stack View for configuration and management purposes.

# 2.4 Stack View (Main Display)

## 2.4.1 Switch Contacted

When Stack View contacts the switch, Stack View shows the front (interface side) of the switch.

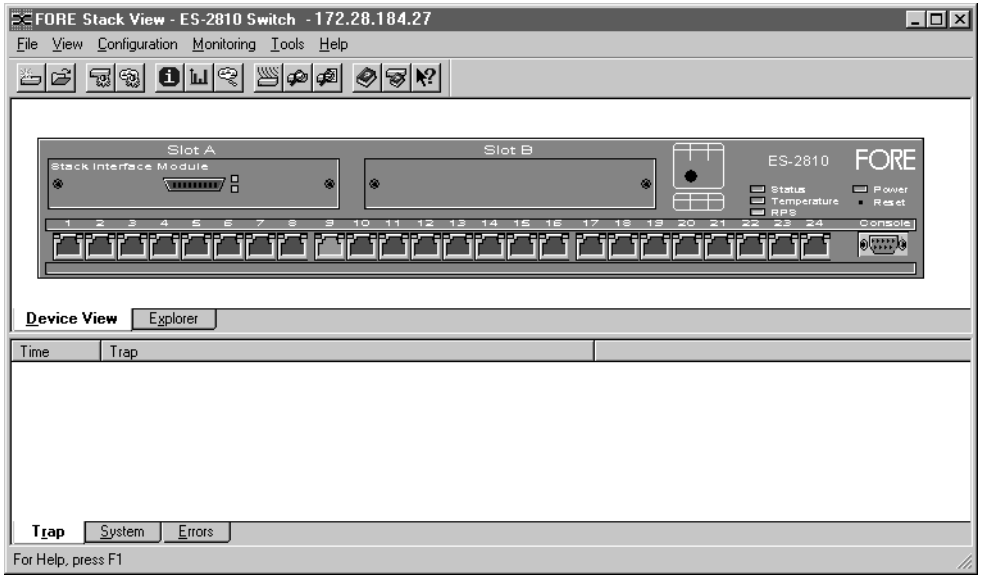



**Figure 2.3 -** View of ES-2810 in Stack View

From this display you can fully manage the switch.

## 2.4.2 Mouse Moves

The use of the mouse will make Stack View easier to use and save you time:

**Table 2.2 -** Mouse Controls in Stack View

| Mouse action | Information |
|---|---|
| Right-click on switch | Shows all the switch-related menus for configuration |
| Right-click on port | Shows all the port-related menus for configuration |
| Double left-click on switch | Shows the Device Setup menu |
| Double left-click on a port | Shows that port's Setup menu |

## 2.4.3 Color Coding

The switch and ports are displayed in different colors:

**Table 2.3 -** Switch and Port Colors in Stack View

| Color | Means |
|---|---|
| Grey | The switch is operational (the software is loaded and running) and it can be contacted by Stack View via the network |
| Black | That port or the switch is selected for further work |
| Blue | Stack View has lost contact with the switch (for example, the switch or your PC is disconnected from the LAN) |
| Dark green | Port enabled, but no plug connected |
| Light green | Port enabled and plug connected |
| Brown | Port disabled by management or a hardware error |

### 2.4.4 Facilities Offered

FORE Systems Stack View offers the following facilities:

- Display of a real-time view of the switch and ports, which behaves in the same way as the physical switch. For example, the LEDs change color according to the state of the switch.
- Total configuration of the switch and ports.
- Backup memory to disk and restore from disk.
- The RAM configuration can be saved to the Flash Memory and subsequently restored to make it the active configuration.
- Detailed monitoring information for each port.

  Other monitoring information ranges from hardware details, such as memory size for the RAM and Flash Memory, to software status information such as how long time the switch has been active since last reboot (also called System up time).
- A comprehensive range of statistics, coupled with powerful graphical facilities, allows you to analyze information by viewing any statistic in isolation or several statistics simultaneously for comparison.
- Remote login from the management host to the Local Management facility of the switch using Telnet. Local Management provides a range of powerful utilities for quick setup, monitoring, software update, diagnostics, and management, which you can fully exploit directly from Stack View.

# 2.5 Setting the Preferences

## 2.5.1 Setting the Polling Intervals

The polling intervals determine how often Stack View contacts the switch and updates the status and information displayed. To change the polling parameters:

1. Select Monitoring>Preferences.

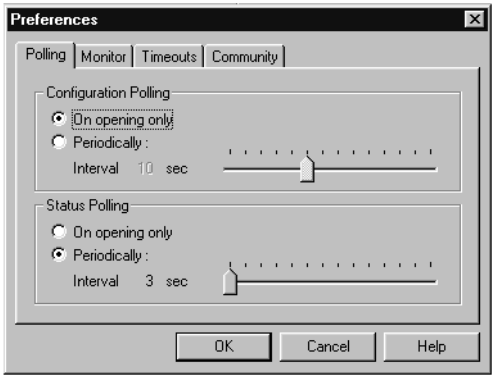



**Figure 2.4 -** Preferences Dialog Box

2. Click **Polling** or **Monitor**.
3. If you want the polling to happen more frequently than just on opening, click **Periodically**.
4. Click the pointer in Interval, and move it to the required time.
5. Click **OK**.

## 2.5.2 Setting the Timeout Parameters for SNMP

The timeout intervals for SNMP determines how often Stack View contacts the monitor and updates the status and information displayed. To change the polling parameters:

1. Select Monitoring>Preferences.
2. Click **`Timeout`**.

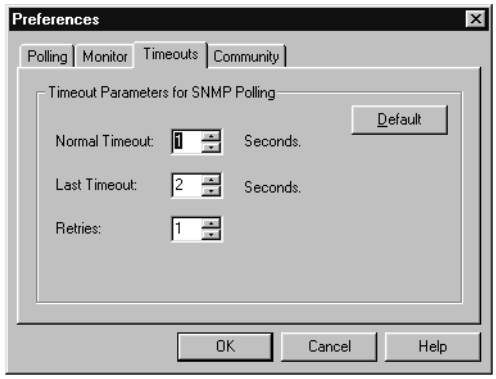



**Figure 2.5 -** Timeout Preferences

3. Change the values
4. Click **`OK`**.

## 2.5.3 Setting the Community for SNMP Polling

The community for SNMP polling determines how often Stack View contacts the monitor and updates the status and information displayed. To change the polling parameters:

1. Select Monitoring>Preferences.
2. Click **`Community`**.

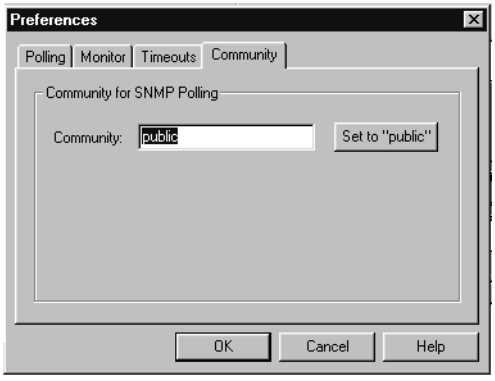



**Figure 2.6 -** Community Preferences

3. Type the new community name.
4. Click **`OK`**.

# 2.6 Menu and Toolbar Overview

The most commonly used facilities from the menus can also be accessed directly from the toolbar, shown in Figure 2.7.

**Figure 2.7 -** Stack View Toolbar

## 2.6.1 File Menu

The File menu contains the following switch facilities:

**Table 2.4 -** File Menu Commands

| Command | Action |
|---|---|
| New | Installs a new switch (which does not have an IP address) in Stack View. A switch can also be installed by pressing the New Device Wizard icon  . |
| Open | Opens Stack View for a switch which has an IP address. A switch can also be opened by pressing the Open Device icon. |
| Close | Closes Stack View for the switch. |
| Save | Saves the software in the switch with its current file name. |
| Save As... | Saves the software in the switch to a location you specify. |
| Create Shortcut | Creates a shortcut icon with the name and IP address of the switch. |
| Exit | Exits the Stack View. If the configuration for the switch has been changed and has not been saved to the Flash Memory as the permanent configuration, you will be asked if you want to save the new configuration before exiting. |
| In addition, the IP addresses of the last 8 switches successfully contacted from Stack View can be opened directly (last switch first) from the File menu. | |

## 2.6.2 View Menu

The View menu allows you to customize the Stack View display to your own preferences:

- Toolbar and Status Bar can be toggled on and off
- Diagnostics and traps can be cleared
- Stack View window can be restored to its original size
- SNMP Trap setup can be changed by selecting the Modify Views icon  .

## 2.6.3 Configuration Menu

This menu allows you to open the configuration tool for the switch—the configuration tool can also be accessed by selecting the Device Setup icon  and to manage configurations for the switch.

## 2.6.4 Monitoring Menu

This menu gives access to extensive monitoring information for the switch and the switch links.

## 2.6.5 Tools Menu

The Tools menu gives access to the following facilities for managing the switch:

- A report manager for uploading reports, logs and the parameter block from the switch—can also be accessed by selecting the Report Manager icon 
- An RMON manager for monitoring the switch using RMON—can also be accessed by selecting the RMON Manager icon 
- Direct access to Local Management on the switch—can also be accessed by selecting the Local Manager icon  .

### 2.6.6 Help Menu

The Help menu gives access to the following help facilities for the switch:

- Help for Stack View—can also be accessed by selecting the About icon . Context sensitive help is available by selecting the Help icon then clicking on the feature of interest.
- A color coding chart for the Stack View to show the states of switch's LEDs.
- The On-line Reference manual for the switch giving detailed concept information about the protocols and features supported by the switch—can also be accessed by selecting the Reference Manual icon .

## 2.7 Stack View Explorer

The Explorer within Stack View allows you to display management information, for example VLANs on the switch.

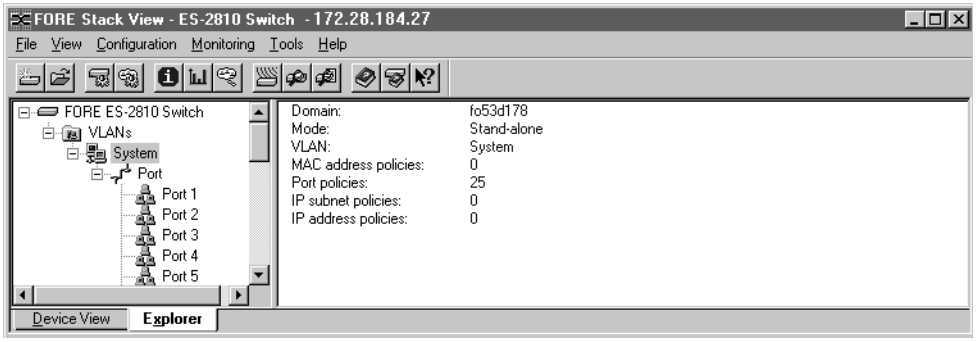



**Figure 2.8 -** Stack View Explorer

If a switch is disabled or not operational, it is displayed with a red cross through it.

General management information for the switch is accessed from the Monitoring menu.

## 2.8 Trap Window

The Traps window displays all traps generated by the switch

### 2.8.1 Color Coding

Traps are generated by the switch for many events, both normal and errors. Traps displayed in Stack View are color coded according to the severity of the trap.

## 2.9 System Window

The System window is a log of all the major switch events with date and times (for example, return to factory default, filter entry settings, modules inserted in slots).

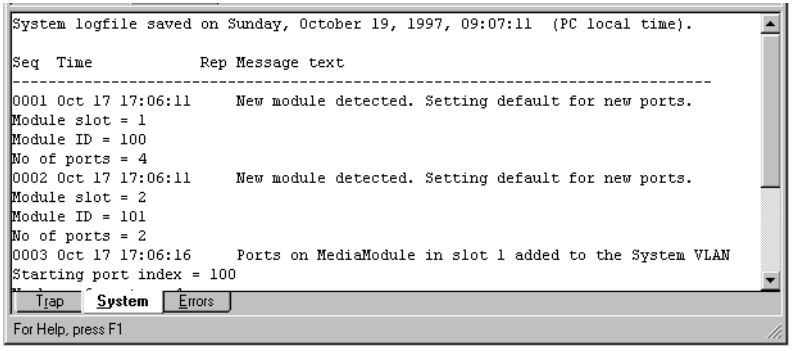



**Figure 2.9 -** System Window Log

# 2.10 Errors Window

The Errors window is a log of all error messages generated by the switch

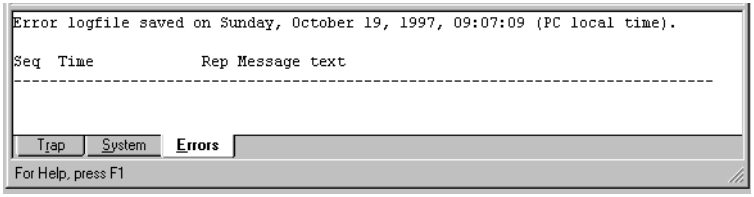



**Figure 2.10 -** Errors Window Log

# CHAPTER 3 Standard Configuration

Configuration is the way we change the setup of the switch. In this chapter you will find all the instructions you need to change setups that affect the switch and the ports.

**Table 3.1 -** Topics in this Chapter

| For Information on This Topic... | Refer to... |
|---|---|
| Changing the Setup of the Switch | page 3-1 |
| Changing the Setup of the Port | page 3-16 |

In chapter 4 you will find instructions to integrate VLANs into your setup.

## 3.1 Changing the Setup of the Switch

### 3.1.1 Improving Switch Security

To restrict the use of the switch using Device Setup, you can:

- Change the administrator password.
- Change the user password.
- Limit access to Local Management via the Console port and / or Telnet.
- Specify a time of “no input”, after which the connection with Local Management is terminated.
- Change the password for moving files with TFTP.
- Specify use of TFTP.
- Restrict access to include only the stations named on the SNMP Authentications list.

## 3.1.2 Using the Mouse

There are three methods of obtaining the Device Setup window:

- Use the pull-down menus
- Double left-click on the switch
- Right-click on the switch

## 3.1.3 System

To assist with switch identification and administration, you can change certain switch details (name, location and contact person):

1. Select Configuration>Device Setup.
2. Click **System**.

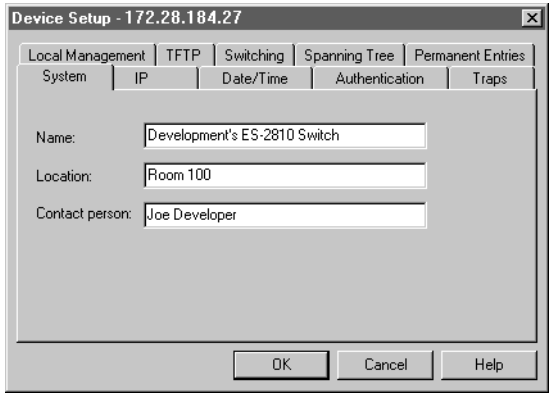



**Figure 3.1 -** Device Setup Dialog Box

3. Change the details.
4. Click **OK**.

   These details are used by SNMP management centers.

## 3.1.4 Switching

### 3.1.4.1 Changing the MAC Address Ageing Time

To change the time a MAC address is kept in the database before being purged:

1. Select Configuration>Device Setup.
2. Click **Switching**.

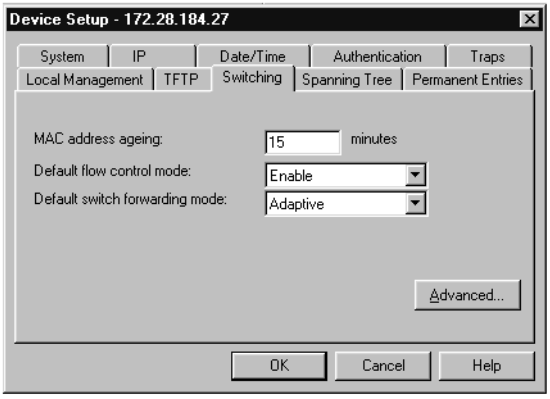



**Figure 3.2 -** Switching Tab of Device Setup Dialog Box

3. Click **MAC Address Ageing**.
4. Type the required number of minutes.
5. Click **OK**.

### 3.1.4.2 Changing the Flow Control

Flow control prevents the loss of frames during busy periods. To change the default flow mechanism on all ports:

1. Select Configuration>Device Setup.
2. Click **Switching**.
3. Click **Default Flow Control**.
4. Click **Enabled**.
5. Click **OK**.

### 3.1.4.3 Changing the Default Forwarding Mode

To change the forwarding mode to be used on all ports:

1. Select Configuration>Device Setup.
2. Click **`Switching`**.
3. Click **`Default Switch Forwarding Mode`**.
4. Click the default forwarding mode you want.
5. Click **`OK`**.

### 3.1.4.4 Adaptive Forwarding Mode

You can:

- Change the Sample Time
- Define the minimum and maximum errors before changing adaptive forwarding mode


While CRC errors and runts are the most likely parameters to cause the switching mode to change, they are not the only ones.

### 3.1.4.5 Changing the Time to Measure Errors

The sample time should be the shortest time needed to detect errors. If the sample time is too great, there may be too many errors before the forwarding mode changes. To change the time the switch retains error counters:

1. Select Configuration>Device Setup.
2. Click **Switching**.
3. Click **Advanced**.

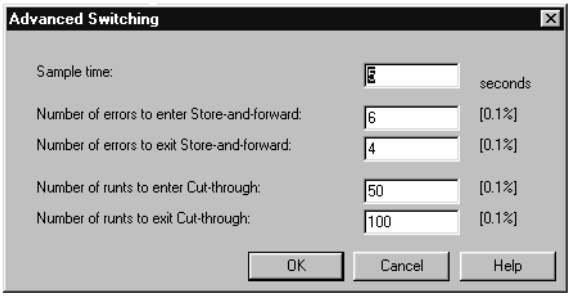



**Figure 3.3 -** Advanced Switching Dialog Box

4. Click **Sample Time**.
5. Type the required number of seconds.
6. Click **OK**.

#### 3.1.4.5.1 Changing Number of Errors Before Adaptive Forwarding Mode Operates

Adaptive forwarding changes the forwarding mode depending on the upper and lower limits of specific error types. To change the number of upper and lower limits:

1. Select Configuration>Device Setup.
2. Click **Switching**.
3. Click **Advanced**.
4. Click the required parameter.
5. Type the number of errors or runts.
6. Click **OK**.

## 3.1.5 Internet Protocol

To change the main IP address and network mask:

1. Select Configuration>Device Setup.
2. Click **IP**.

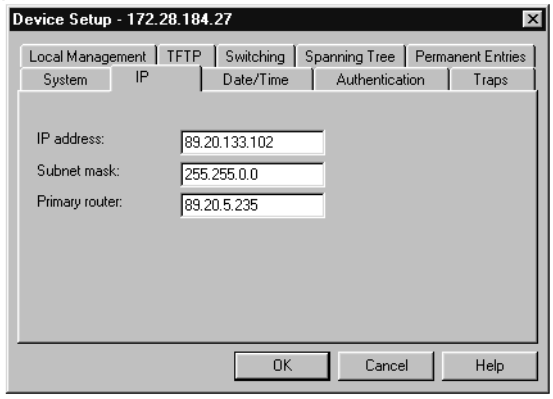



**Figure 3.4 -** IP Tab of Device Setup Dialog Box

3. Change the details.
4. Click **OK**.

   These details are used by SNMP management centers.

## 3.1.6 Spanning Tree

You can change the:

- Priority given to the switch
- Maximum length of time information is retained by the switch
- Time between transmitted Configuration BPDUs
- Time the switch spends in the Listening and Learning states

### 3.1.6.1 Warning when using VLANs

It is important to be aware of problems that may arise when using Spanning Tree and VLANs. The Spanning Tree can use alternative paths (such as different ports) to get messages to their destination. VLANs specify which ports can receive messages.

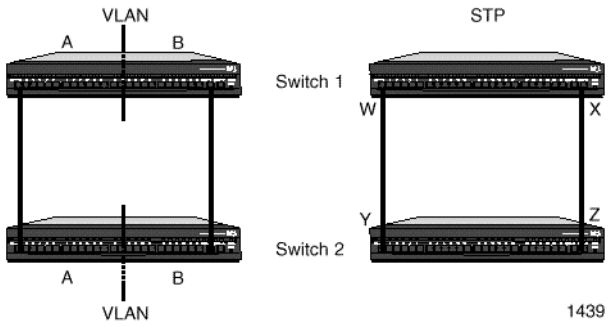



**Figure 3.5 -** Configuration with Spanning Tree Protocol

In the above diagram, we have two switches. To the left, we see the two switches connected and the ports are grouped in two VLANs: A and B. On the right, we have enabled STP; STP blocks the path between X and Z (to avoid looping) and, therefore, destroys the VLAN setup (because the VLAN needs these ports to receive messages).

### 3.1.6.2 Why Change These from their Defaults?

The switch is delivered with Spanning Tree default values set to those recommended by the IEEE 802.1D standard. These values are conservative "worst-case" estimates for LANs consisting of a large number of switches. Because of your network configuration, changing these default values may improve network performance.

### 3.1.6.3 Changing the Spanning Tree Priority

The higher the value, the lower the chance of the switch being used as the root bridge. To change the priority value:

1. Select Configuration>Device Setup.
2. Click Spanning Tree.

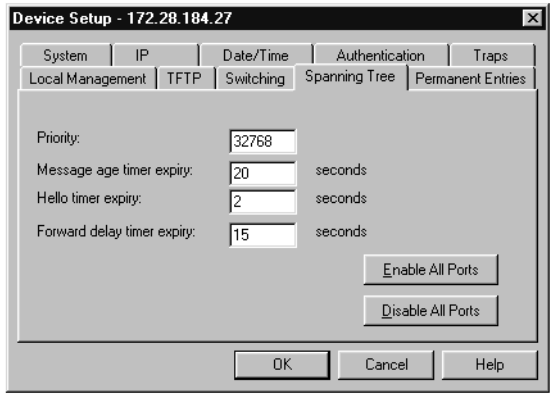



**Figure 3.6 -** Spanning Tree of Device Setup Dialog Box

3. Click **Priority**.
4. Type the required value.
5. Click **OK**.

### 3.1.6.4 Changing the Message Age Expiry Time

To change the maximum time between protocol information being received and discarded:

1. Select Configuration>Device Setup.
2. Click **Spanning Tree**.
3. Click **Message Age Timer Expiry**.
4. Type the required number of seconds.
5. Click **OK**.

### 3.1.6.5 Changing the Hello Expiry Time

To change the time between transmissions of configuration BPDUs from a switch that is, or attempting to become, the root:

1. Select Configuration>Device Setup.
2. Click **Spanning Tree**.
3. Click **Hello Timer Expiry**.
4. Type the required number of seconds.
5. Click **OK**.

### 3.1.6.6 Changing the Forward Delay Expiry Time

To change the time between port states while the bridge attempts to become the root:

1. Select Configuration>Device Setup.
2. Click **Spanning Tree**.
3. Click **Forward Delay Timer Expiry**.
4. Type the required number of seconds.
5. Click **OK**.

### 3.1.6.7 Changing the State of the Ports

To specify that all ports are using Spanning Tree Protocol:

1. Select Configuration>Device Setup.
2. Click **Spanning Tree**.
3. Click **Enable All Ports**.

   The ports are able to resolve problematic network loops using STP.
4. Click **OK**.

## 3.1.7 Authentication

SNMP is a fully defined, interoperative standard which helps you manage both the switch and the network. To do this you can:

- Specify the names of the hosts to access the SNMP agent on the switch (authentication) by defining the source IP and community
- Specify Read-Write or Read-Only for authenticated hosts
- Request a trap to be sent if authentication is violated


If no hosts are defined in the Authentication List, any host can access the SNMP agent in the switch.

### 3.1.7.1 Security

The authentications list defines the hosts that can carry out SNMP, TFTP or Telnet management on the switch, have read-write or read only rights and access to communities. You can:

- Add a new entry to the list
- Delete an entry
- Edit existing entries

### 3.1.7.2 Adding a Device

To add a host that is allowed to carry out SNMP management on the switch:

1. Select Configuration>Device Setup.
2. Click **`Authentications`**.

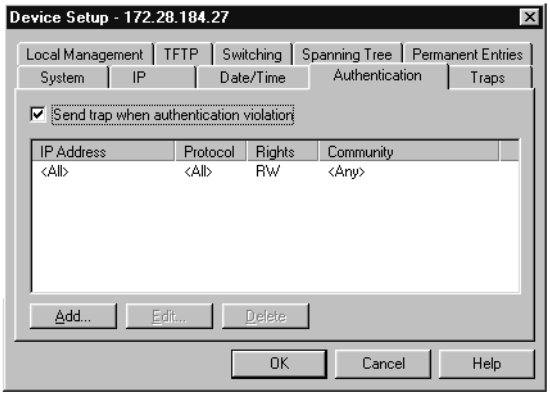



**Figure 3.7 -** Authentication Tab of Device Setup Dialog Box

3. Click **`Send trap when authentication violation`**.

   A message will be sent to the Traps window if unauthorized hosts try to carry out SNMP management on the switch.

4. Click **`Add`**.
5. In `IP address`, type the IP address of the device to manage the switch.

   You can have a maximum of eight addresses in the list. The address 0.0.0.0 shows all IP addresses are accepted.

6. Click **`Protocol`**, and select one.
7. Click **`Rights`**, and specify the level of access to the SNMP agent
8. Click **`Community`**, type the SNMP request name accepted by the SNMP agent.

   If no community name is specified, all community names are accepted by the SNMP agent.

9. Click **`OK`**.

## 3.1.8 Traps

A trap alerts you of the changes that occur in the SNMP agent system. The traps list shows where SNMP traps (generated by the switch) are sent. You can:

- Add a new entry to the list
- Delete an entry
- Edit existing entries

### 3.1.8.1 Adding a Trap

**NOTE** If there are no entries in the Traps list, there are no SNMP traps sent.

1. Select Configuration>Device Setup.
2. Click **Traps**.

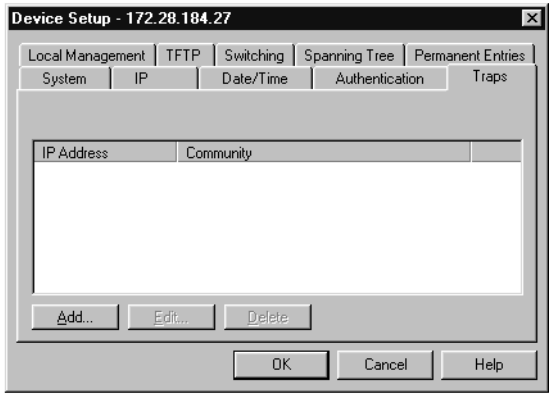



**Figure 3.8 -** Traps Tab of Device Setup Dialog Box

3. Click **Add**.
4. Type the Destination IP address, or click **This PC**.
5. Type the community (SNMP password).
6. Click **OK**. This has now been saved.

## 3.1.9 Local Time

To change the clock in the switch to your local time:

1. Select Configuration>Device Setup.
2. Click **Date/Time**.

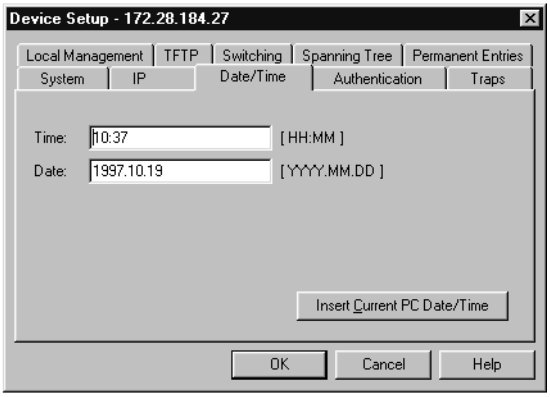



**Figure 3.9 -** Date / Time Tab of Device Setup Dialog Box

3. Click **Insert Current PC Date/Time** to show the present settings. If this is satisfactory, click **OK**.

**NOTE** The clock displays the time that it is accessed and not the current time.

4. If the time or the date is not satisfactory, click in the fields and type the new time and date.
5. Click **OK**.

## 3.1.10 Local Management

### 3.1.10.1 Changing Password Details

The administrator has read-write access at all levels. The user can read the monitoring screens, but is not allowed to change the configuration, update software or reset the station. To prevent unauthorized personnel changing configurations:

1. Select Configuration>Device Setup.
2. Click **`Local Management`**.

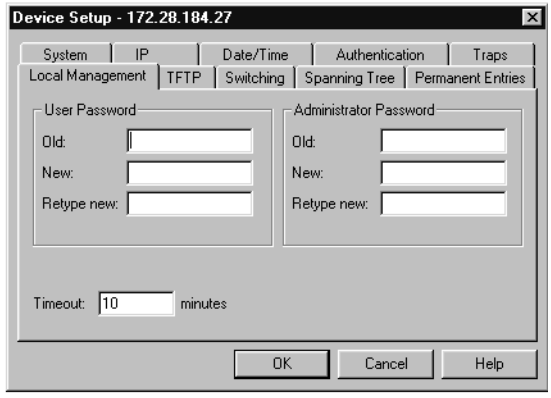



**Figure 3.10 -** Local Management Tab of Device Setup Dialog Box

3. Select the password you want to change.
4. Type the old password.
5. Type the new password.
6. Again, retype the new password (in `Retype new`).
7. Select **`OK`**.

### 3.1.10.2 Changing Timeout Details

When there has been no input during this period, the connection with Local Management is terminated. To change the interval.

1. Select Configuration>Device Setup.
2. Click **`Local Management`**.
3. Type the new time.
4. Select **`OK`**.

## 3.1.11 TFTP

### 3.1.11.1 Changing Password Details

To give added security, you can limit the number of staff authorized to transfer TFTP files by changing the TFTP password. To change the password.

1. Select Configuration>Device Setup.
2. Click **`TFTP`**.
3. Type the old password.
4. Type the new password.
5. Again, type the new password (in `Retype new`).
6. Select **`OK`**.

## 3.2 Changing the Setup of the Port

You can configure the port to operate in different ways—according to your network's requirements:

- Change the port state
- Select the auto-negotiation mode
- Change each port to half or full duplex

  If not enabled by auto-negotiation
- Specify the speed of the port

  If not enabled by auto-negotiation
- Change the forwarding mode of the port
- Change the flow control setting of the port

### 3.2.1 Using the Mouse

There are three methods of obtaining the Device Setup window:

- Use the pull-down menus
- Double left-click on the port
- Right-click on the switch

## 3.2.2 General Changes

### 3.2.2.1 Renaming a Port

To give a port a new name, for example, its use or the user(s) connected:

1. Click the port you want to rename.
2. Select Configuration>Port Setup.
3. Click **General**.

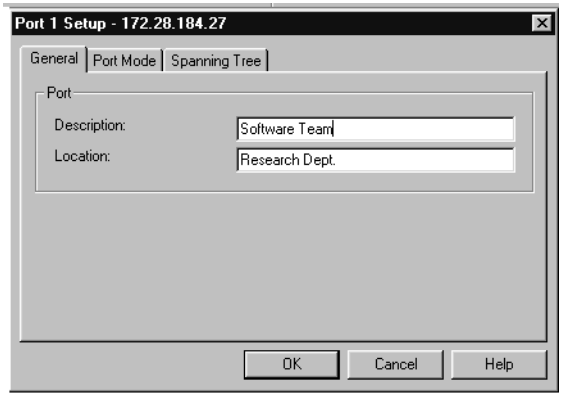



**Figure 3.11 -** General Tab of Port Setup Dialog Box

4. Click in the Description field.
5. Type the new name.
6. Click **OK**.

### 3.2.2.2 Location for a Port

To specify the location (for example, an office number or department) of the device attached to a port:

1. Click the port you want to give a home to.
2. Select Configuration>Port Setup.
3. Click **General**.
4. Click in the Location field.
5. Type where the device is.
6. Click **OK**.

## 3.2.3 Port Mode

### 3.2.3.1 Disabling the Port

If you disable the port, the devices attached to it cannot use the switch. The MAC address of those devices are removed from the switch's address table after the MAC address ageing time has elapsed. If those addresses are defined as permanent entries, they are not purged. To disable the port:

1. Click the port you want to disable.
2. Select Configuration>Port Setup.
3. Click **`Port Mode`**.

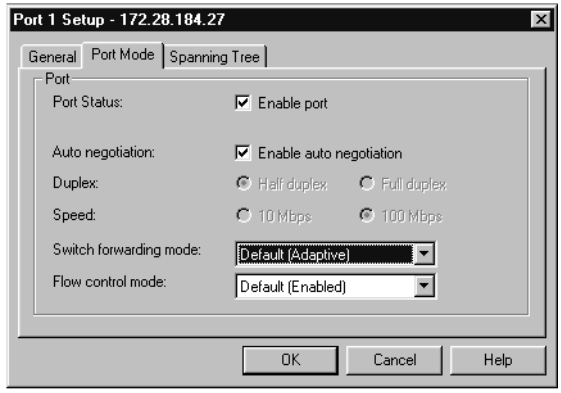



**Figure 3.12 -** Port Mode Tab of Port Setup Dialog Box

4. Click **`Enable Port`**.

   If there is a check mark is in the box, the port is operational. If the box is empty, the port is disabled.

5. Click **`OK`**.

### 3.2.3.2 Disabling Auto-negotiation

To disable auto-negotiation, and reset the speed to the values specified in Speed:

1. Click the port you want to disable.
2. Select Configuration>Port Setup.
3. Click **Port Mode**.
4. Click **Enable Auto-negotiation**.

   If there is a check mark is in the box, the port automatically detects the line-speed and duplexity. If the box is empty, auto-negotiation is disabled and the port uses the values specified in Duplex and Speed.
5. Click **OK**.

### 3.2.3.3 Changing Duplex Mode

To change the port's duplex mode (when auto-negotiation is disabled):

1. Click the port you want to change.
2. Select Configuration>Port Setup.
3. Click **Port Mode**.
4. Click **Half Duplex** or **Full Duplex**.

   Half allows either transmission or receipt of the data and Full allows both transmission and receipt of the data.
5. Click **OK**.

### 3.2.3.4 Changing the Port Speed

To change the speed at which a port can accept data (when auto-negotiation is disabled):

1. Click the port you want to change.
2. Select Configuration>Port Setup.
3. Click **Port Mode**.
4. Click **Speed 10** or **Speed 100**.

   10 limits data entering to 10Mbps and 100 allows data speeds up to 100Mbps.
5. Click **OK**.

### 3.2.3.5 Changing the Forwarding Mode on a Port

To change the forwarding mode to be used on a port:

1. Click the port you want to change.
2. Select Configuration>Port Setup.
3. Click **`Port Mode`**.
4. Click in the `Switch Forwarding Mode` field.
5. Click the forwarding mode you want.

   Default is the same forwarding mode as specified in Configuration>Device Setup.
6. Click **`OK`**.

### 3.2.3.6 Changing the Flow Control on a Port

Flow control prevents the loss of frames during busy periods. To change the flow mechanism on a port:

1. Click the port you want to change.
2. Select Configuration>Port Setup.
3. Click **`Port Mode`**.
4. Click **`Flow Control`**.
5. Click the flow control you want.

   Default is the same flow control as specified in Configuration>Device Setup.
6. Click **`OK`**.

## 3.2.4 Port Specific Spanning Tree

You can:

- View the Spanning Tree setups for all ports
- Specify which ports are in the STP (Spanning Tree Protocol)
- Define which ports are going to be used most frequently
- Specify all ports to participate in STP
- Specify none of the ports to participate in STP

### 3.2.4.1 Changing the State of a Port

To specify that a port is using STP:

1. Click the port you want to change.
2. Select Configuration>Port Setup.
3. Click **Spanning Tree**.

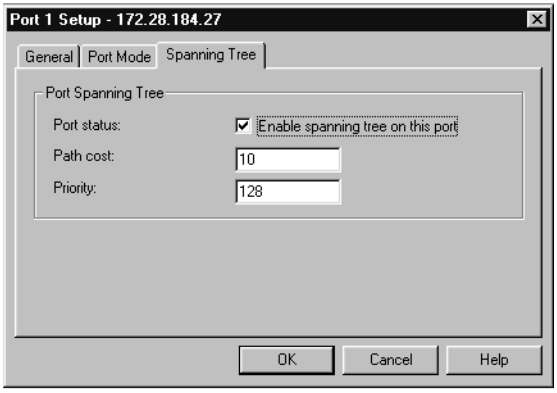



**Figure 3.13 -** Spanning Tree Tab of Port Setup Dialog Box

4. Click **Enable spanning tree on this port**.

   If there is a check mark in the box, the port is used in STP. If the box is empty, the port is not used in STP.

5. Click **OK**.

### 3.2.4.2 Changing the Cost of the Path

The higher the cost, the lower the chance of this port being used in STP. When possible, give a port a low cost if it is connected to a faster network segment. To change the overall cost of the path between a port and the root port:

1. Click the port you want to change.
2. Select Configuration>Port Setup.
3. Click **Spanning Tree**.
4. Click **Path cost**.
5. Type the required value.
6. Click **OK**.

### 3.2.4.3 Changing Priority of the Port in the Spanning Tree

The higher the value, the lower the chance of this port being used as the designated or root port. To change the priority value:

1. Click the port you want to change.
2. Select Configuration>Port Setup.
3. Click **Spanning Tree**.
4. Click **Priority**.
5. Type the required value.

   If there are two ports with the same value, the port with the lowest port number will be chosen.
6. Click **OK**.

# CHAPTER 4 Advanced Configuration

In this chapter you will learn how to use Advanced Configuration effectively. This chapter covers VLANs (Virtual LANs).

Create logical network groups (Virtual LANs) by segmenting the switch, for example according to the subnetting scheme within your network. Each VLAN is an isolated group and the switch only forwards traffic between members of the same group. Communication between groups can be implemented using routers.

## 4.1 VLANs (Virtual LANs)

Configuring VLANs allows you to:

- Create up to 128 separate user groups
- Limit broadcast and multicast traffic
- Increase security by limiting communication between groups
- Allocate network resources (such as servers) to groups

For a more comprehensive explanation of the VLAN concept, refer to Appendix A.

### 4.1.1 Warning When Using STP

It is important to be aware of problems that may arise when using Spanning Tree and VLANs. The Spanning Tree can use alternative paths (such as different ports) to get messages to their destination. VLANs specify which ports can receive messages.

***WARNING!***

When using the Spanning Tree facility, only use one VLAN. If you do use two or more VLANs, this may cause unexpected changes in your network topology.

## 4.1.2 Policy-based VLANs

This switch uses “Policy-based VLANs”. This means that the devices attached to the switch can be grouped by any combination of MAC address, IP address, IP subnet and port number; therefore, devices can belong to one or more VLANs.

## 4.1.3 Policy Hierarchy

If there is a conflict between two VLANs, there is a strict order of priority for the policies:

1. MAC address
2. IP address and IP Subnet and Mask
3. Switch ports

***WARNING!***

If a station belongs to a VLAN with a high priority policy (for example, MAC address), then it cannot belong to another VLAN using a policy with a lower priority (for example, port).

## 4.1.4 Adding a VLAN

This task of adding VLANs is simplified by using the VLAN Wizard. To add a VLAN:

1. Select Configuration>VLAN Setup.

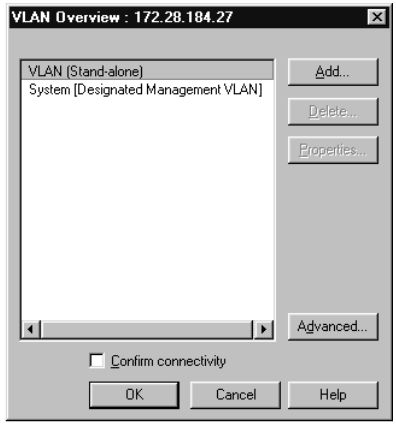



**Figure 4.1 -** VLAN Overview Dialog Box

2. Click **Add**, and follow the instructions in the Wizard windows.

**Table 4.1 -** Information Required for VLAN Policies

| Policy | Information required |
|---|---|
| Switch Ports | Port numbers |
| IP Subnet | IP Subnet and Mask |
| Multipolicy | IP Subnet and Mask,<br>Port numbers,<br>MAC address and / or<br>IP address |

## 4.1.5 Deleting a VLAN

To delete a VLAN:

1. Select Configuration>VLAN Setup.
2. Click the name of the VLAN you want to delete.

   Note: you cannot delete this VLAN if it is the `[Designated Management VLAN]`. To do this:

   a. Click another VLAN, click **`Properties`**.

   b. Click **`Use this VLAN for SNMP management`**.

   c. Now delete the first VLAN.
3. Click **`Delete`**.

## 4.1.6 Changing the Name of a VLAN

To change the name of a VLAN:

1. Select Configuration>VLAN Setup.
2. Click the name of the VLAN you want to delete.
3. Click **`Properties...`** The VLAN name is highlighted.
4. Type the new name VLAN Name.
5. Click **`Close`** to accept the name.

## 4.1.7 Ports with IP Learning

If you have ports on which you only have IP traffic, then you can use the IP rules. You must specify this. Port and MAC learning will still be used. Within the VLAN, there are some ports that you want to use IP only—not ports or MAC addresses. To specify those ports:

1. Select Configuration>VLAN Setup.
2. Click the name of the VLAN you want to change.
3. Click **Advanced...**.
4. Click **IP Traffic...** to see the ports that only use IP.

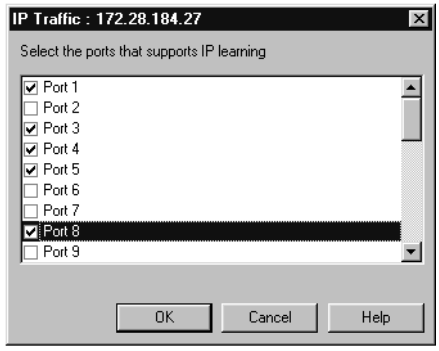



**Figure 4.2 -** IP Traffic Dialog Box

If there is a check mark in the box, the port only uses IP. If the box is empty, the port uses all protocols.

5. Click **OK**.

# CHAPTER 5 Managing the Switch



This chapter covers the topics listed in Table 5.1.

**Table 5.1 -** Topics in this Chapter

| For Information on This Topic... | Refer to... |
|---|---|
| Monitoring the Switch's Performance | page 5-2 |
| Monitoring the Port's Performance | page 5-6 |
| Tools for the Switch | page 5-10 |

## 5.1 Management Using Stack View

### 5.1.1 Why use Stack View?

Stack View allows you to:

- Use the Switch Manager to:
  - Configure system, switching, IP, spanning tree, authentication, and trap parameters for the switch.
  - Configure port-related parameters.
  - View traps, logs, traces, and reports generated by the switch.
  - Monitor port activity.
  - Monitor port faults.
  - Monitor switch activity.
- Use the RMON Manager to:
  - Gather information about network traffic.
  - Monitor traffic on a subnet.
  - Define your own alarm thresholds.

# 5.2 Monitoring the Switch's Performance

## 5.2.1 Monitoring the Total Packet Activity

To view the total activity of the packets on all the ports:

1. Select Monitoring>Device Activity>Total Packets...

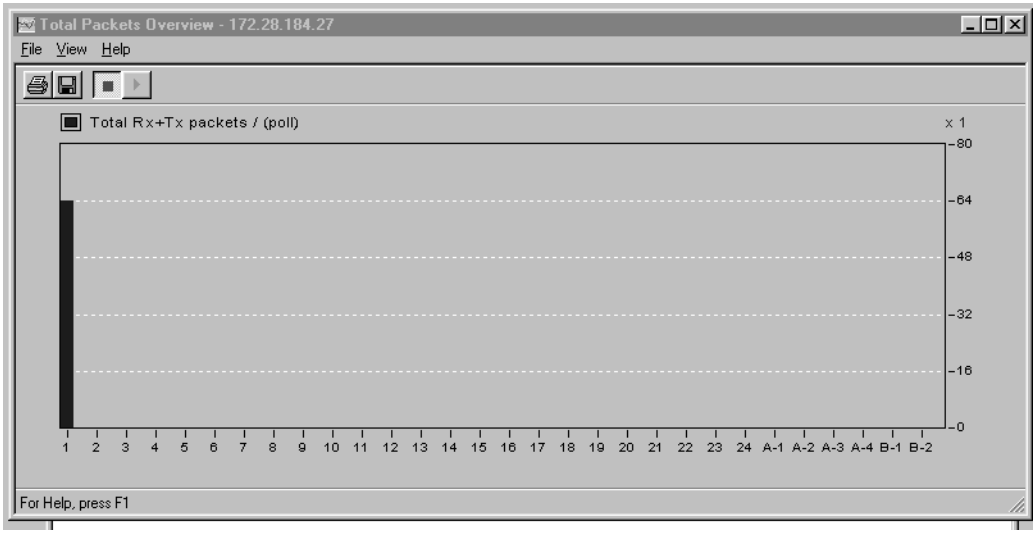



**Figure 5.1 -** Total Packets Overview

Each column represents a port and its activity level.

2. Right-click a port, and select **`Common Scaling`**, **`Freeze Y-axis`**, **`Stop collection`**, **`Print`** or **`Change Colors`** from the popup menu.

## 5.2.2 Monitoring the Total Activity of Transmitted Packets

To view the total activity of the packets being transmitted on all the ports:

1. Select Monitoring>Device Activity>Tx Packets...

   Each column represents the activity level on that port.

2. Right-click a port, and select **`Common Scaling`**, **`Freeze Y-axis`**, **`Stop collection`**, **`Print`** or **`Change Colors`** from the popup menu.

## 5.2.3 Monitoring the Total Activity of Received Packets

To view the total activity of the packets being received on all the ports:

1. Select Monitoring>Device Activity>Rx Packets...

   Each column represents the activity level on that port.

2. Right-click a port, and select **`Common Scaling`**, **`Freeze Y-axis`**, **`Stop collection`**, **`Print`** or **`Change Colors`** from the popup menu.

## 5.2.4 Monitoring the Total Number of Errors

To view the total error activity of the packets on all the ports:

1. Select Monitoring>Device Activity>Errors...

   Each column represents the activity level on that port.

2. Right-click a port, and select **`Common Scaling`**, **`Freeze Y-axis`**, **`Stop collection`**, **`Print`** or **`Change Colors`** from the popup menu.

## 5.2.5 Monitoring the Spanning Tree Statistics

To view the spanning tree statistics for the whole switch, select Monitoring> nning Tree Statistics.

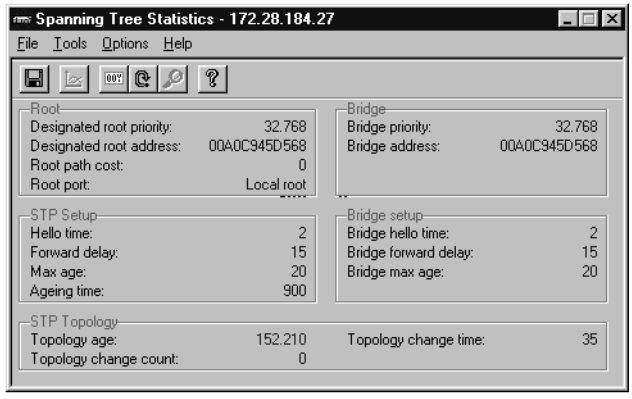



**Figure 5.2 -** Spanning Tree Statistics

## 5.2.6 Overview of All the Ports

To view the setups of all the ports on the switch:

1. Select Monitoring>Port Overview...

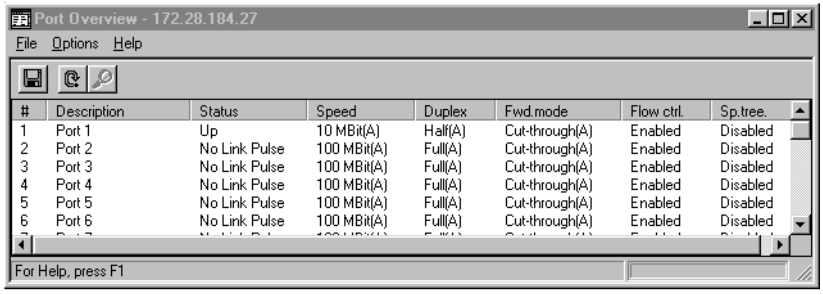



**Figure 5.3 -** Port Overview

2. Double-click a port to get the specific details on port performance, faults, packet distribution and spanning tree information for that port.

## 5.2.7 Overview of the VLANs

To view the VLANs on the switch:

1. Select Monitoring>VLAN Monitoring...

   This shows a full list of VLANs active on the switch. This window is also viewed from the Explorer by right-clicking the VLAN name and selecting **`Monitor...`**

2. Click the name of the VLAN, then click **`Details`** to view details of that VLAN.

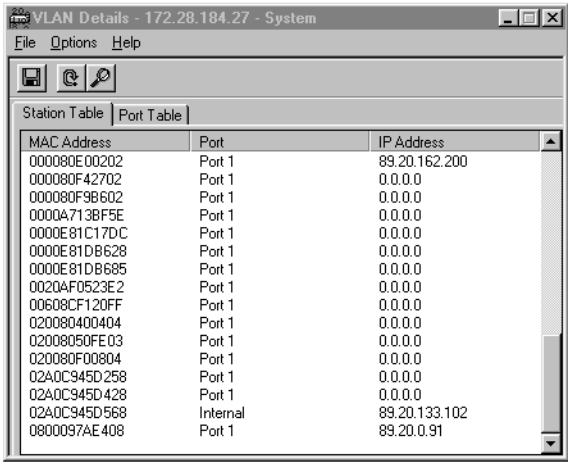



**Figure 5.4 -** VLAN Details

Click on either of the tabs to view more details, as shown in Table 5.2.

**Table 5.2 -** Viewing Detailed VLAN Information

| Tab Name | Shows the VLANs... | Double-click a row to show... |
|---|---|---|
| Station Table | MAC addresses,<br>Ports and<br>IP addresses | all VLANs in which this address is contained |
| Port Table | Port number and<br>Port name | the MAC and IP address of all devices on the port in this VLAN |

# 5.3 Monitoring the Port's Performance

## 5.3.1 Using the LEDs

On the Switch Manager's picture of the switch, the different colors on the ports indicate the different states of activity. Select Help>Display Legend for further information on LED states.

## 5.3.2 Monitoring the Performance of a Port

To monitor the performance of a specific port:

1. Click the port.
2. Select Monitoring>Port Details...>Port Performance....

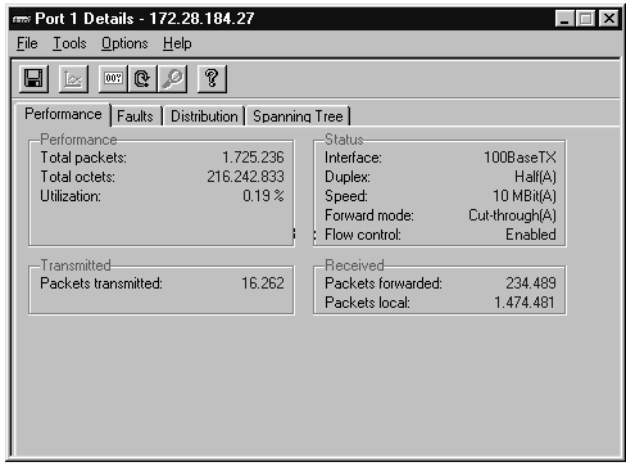



**Figure 5.5 -** Port Details

This table shows the total number of frames and octets, utilization of the ports and the number of packets transmitted and received.

3. To change the display from numerical to graphical, click on one or more of the numbers and select Tools>Graph.

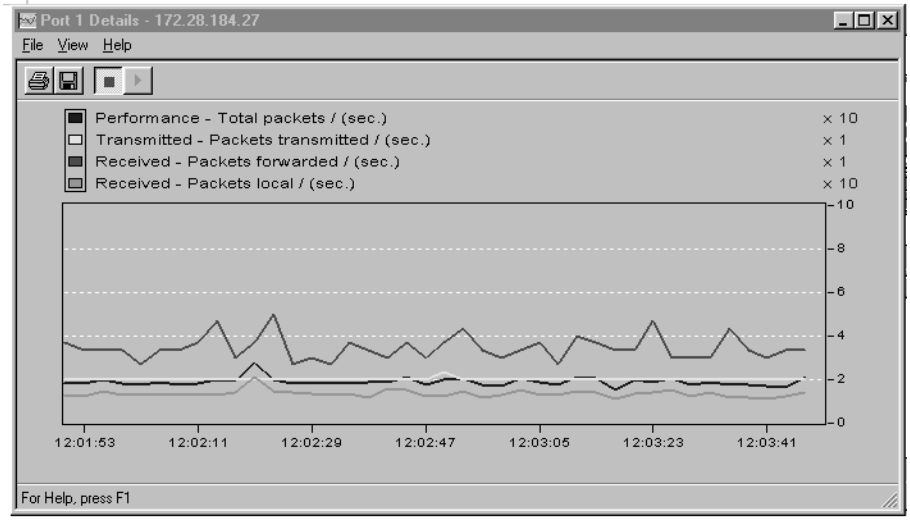



**Figure 5.6 -** Port Details Graphs

4. Select Options>Reset Counters to set all these counters to zero.

## 5.3.3 Monitoring the Faults on a Port

To monitor the faults on a specific port:

1. Click the port.
2. Select Monitoring>Port Details...>Faults.

   This table shows the total number errors, discards and observations transmitted and received.
3. To change the display from numerical to graphical, click on one or more of the numbers and select Tools>Graph.
4. Select Options>Reset Counters to set all these counters to zero.

## 5.3.4 Monitoring the Distribution on a Port

To monitor the distribution percentages of unicast, multicast and broadcast frames on a specific port:

1. Click the port.
2. Select Monitoring>Port Details...>Distribution.

## 5.3.5 Monitoring the Spanning Tree Statistics on a Port

To monitor the spanning tree statistics on a specific port:

1. Click the port.
2. Select Monitoring>Port Details...>Spanning Tree.

## 5.3.6 Monitoring the Received Packets on a Port

To monitor the received packets on a specific port:

1. Click the port.
2. Select Monitoring>Port Activity...>RX... Packets.
3. Select View>Stop Collection, followed by File>Print to print the graph.

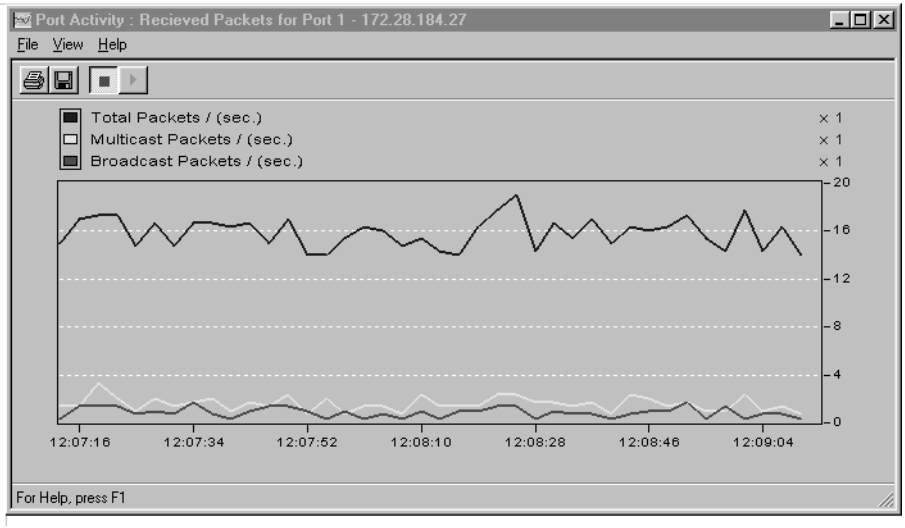



**Figure 5.7 -** Received Packets on Port 1

## 5.3.7 Monitoring the Packets Transmitted from a Port

To monitor the transmitted packets on a specific port:

1. Click the port.
2. Select Monitoring>Port Activity...>TX Packets....
3. Select View>Stop Collection, followed by File>Print to print the graph.

## 5.3.8 Monitoring the VLANs on a Port

To view the VLANs on the port:

1. Select Monitoring>VLAN Port Monitoring...

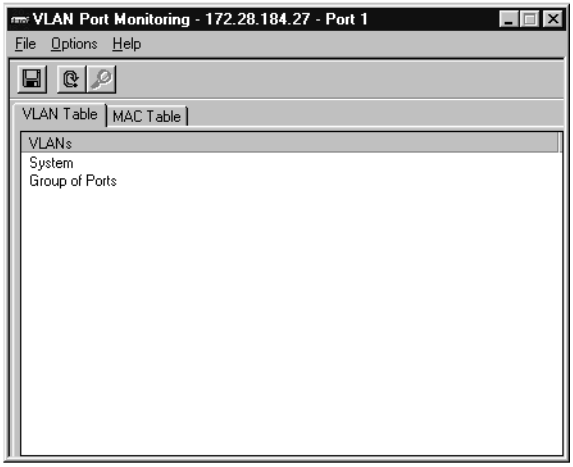



**Figure 5.8 -** VLAN Port Monitoring

2. Click on either of the tabs to view details of that port:

**Table 5.3 -** Viewing Detailed Port Information

| Tab Name | Shows the VLANs... | Double-click a row to show the... |
|---|---|---|
| VLAN Table | in which this port is contained | MAC addresses learned on this port in that specific VLAN |
| MAC Table | MAC addresses and IP addresses | other VLANs in which this address is contained |

# 5.4 Tools for the Switch

## 5.4.1 Tools Available

The switch has various tools to help with management, shown in Table 5.4.

**Table 5.4 -** Management Tools

| Use... | To... |
|---|---|
| Report Manager | Transfer files from a remote switch to your local disk or file server. |
| RMON Manager | Collect details about network traffic. |

## 5.4.2 Report Manager

### 5.4.2.1 Using the Report Manager

To view a log or report:

1. Select Tools>Report Manager.

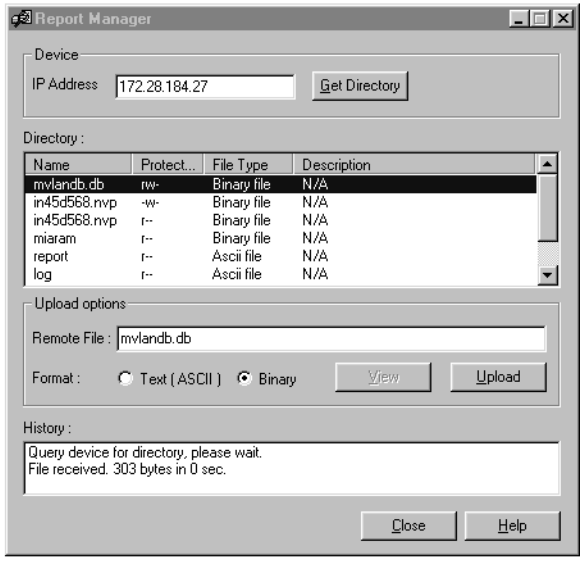



**Figure 5.9 -** Report Manager Dialog Box

2. Double-click IP Address, and type the correct IP address for the device you want to receive the directory.
3. Select a directory from the Directory list box, and click **View**.

## 5.4.3 RMON Manager

### 5.4.3.1 What is a Probe?

The switch contains an RMON probe. The probe is a highly sophisticated tool for collecting information about network traffic.

### 5.4.3.2 Find a Probe on the Switch

To access the probe in the switch, click the RMON Manager icon on the tool bar of the Switch Manager.

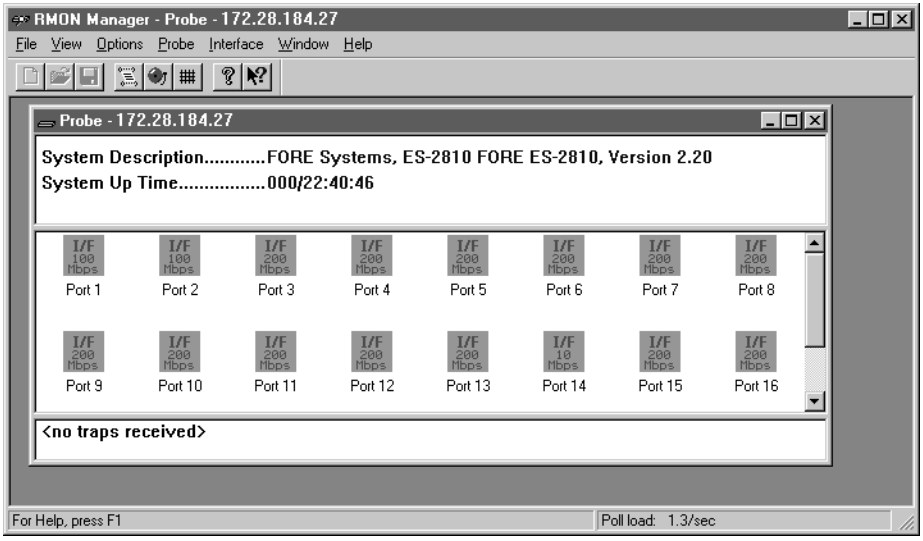



**Figure 5.10 -** RMON Manager Probe

### 5.4.3.3 What you see in the RMON Window

The main window of the RMON Manager contains the following views:

- An information view with a short description of the probe.
- An interface view with the interfaces shown as icons.
- A trap view showing SNMP traps received from the probe.

### 5.4.3.4 Supported Functions

The following RMON functions are supported:

- Interface statistics (including Vital Statistics graph)
- History
- Alarms
- Event

#### 5.4.3.4.1 Interface Statistics

To determine the total amount of traffic on a subnet, double-click the icon representing the interface to the subnet in the Probe window. This opens the Vital Statistics window.

To print the graph, you must first click the red Stop icon in the tool bar to stop the graph activity, and then click the Printer icon.

#### 5.4.3.4.2 Further Interface Statistics

To access a wider range of subnet management statistics:

1. Right-click the interface icon in the Probe window. This opens the interface popup menu.
2. Select Statistics. This window gives more detailed information about the subnet in the form of counters.
3. To view the counters in a graph, select a number of counters by double-clicking them, and click the Graph icon in the tool bar.

#### 5.4.3.4.3 History

To monitor traffic on a subnet over a period of time:

1. Open the History Overview window by pressing the History icon in the main tool bar of the Probe window. This opens a window listing all history collections.
2. To open a graph showing the statistics, select a history and press **Graph**...
3. Select from one to four counters for presentation in a graph from the History Graph Setup window, and press **OK**.

### 5.4.3.5 Alarms

Alarm is a useful feature in the RMON Manager; it enables you to set your own thresholds for when the network activity requires some attention.

1. Press the Alarm icon in the main tool bar. This opens the Alarm Overview window, which lists all alarms defined in the probe.
2. Click **Add...** to add an alarm to the list.

   After defining the alarm, a trap will be sent every time the threshold is exceeded. This trap will automatically be shown in the trap part of the Probe window.

   The example above will cause the probe to issue an alarm if the number of sent errors on interface #12 exceeds 20 or more errors over a period of 15 seconds. When the trap is issued, an RMON log entry may inserted, and an SNMP trap may be sent.


For the RMON Manager to be able to receive traps, it must first be defined as a trap receiver in the probe.

### 5.4.3.6 On-line Help

For further information about the use of the RMON Manager and its facilities, please refer to the extensive on-line Help.

### 5.4.3.7 Command Line Start-up

The RMON Manager can also be started from the command line:

1. Open a command prompt.
2. At the prompt you can enter the following commands:

   **RMONMGR [IP=**<*IP address*>**] [COMM=**<*SNMP community*>**] [ALIAS=**<*probe alias*>**] [NEWDLG]**

   Depending on the entered command, the RMON Manager is started either with a blank program window, an existing probe window or the NEW RMON probe dialog.

   Example: Assume that you want to manage a switch with the community name `production`, the IP address 101.102.103.104, and the switch name `Production_switch`, then the command entered in the command line is as follows:

   RMONMGR IP=101.102.103.104 COMM=production ALIAS=Production_switch

## 5.4.4 Local Management

### 5.4.4.1 Purpose

The main features of the switch's Local Management facility are:

- It can be accessed from any workstation on the network using Telnet
- Access can be password protected to exclude unauthorized personnel
- Two distinct levels of management rights, administrator and user
- Log files (to pinpoint trouble sources) to provide diagnostic information for troubleshooting
- Detailed system information and operational statistics

### 5.4.4.2 What Does It Do?

The switch's ASICs (Application-Specific Integrated Circuits) and support for RMON provide complete management without compromising the switch's performance.

The management facility is divided into four parts:

- Configuration

  Allows you to change the basic configuration parameters of the switch.
- Monitoring shows:
  - A hardware and software overview
  - Details on messages from the system log
  - Normal traffic throughput
  - Number of errors, discards, observations and collisions for the switch
  - An overview of port specific errors, discards, observations and collisions
  - Spanning Tree Protocol for the switch bridge and specific ports
  - MAC addresses on specific ports, and which ports have no MAC addresses
- Diagnostics shows:
  - A log of errors due to software and hardware failures
  - How to overcome the limitations which exist in some management applications (RMON)
  - The option to reset all the counters being used for diagnostic purposes

- Software Update lets you:
  - Load new software to the switch
  - Reset the switch if necessary
  - Monitor the software status

### 5.4.4.3 Access to the Local Management Application

Instructions on how to access the application have been mentioned earlier:

- Access from the CONSOLE port

  Details are in *Quick Start*.
- Access using Telnet

  Select Tools>Local Management...

### 5.4.4.4 Finding the Details

After a successful login, the Local Management main menu is displayed:


**Figure 5.11 -** Local Management Interface

# CHAPTER 6 Technical Specifications

This chapter covers the topics listed in Table 6.1.

**Table 6.1 -** Topics in this Chapter

| For Information on This Topic... | Refer to... |
|---|---|
| Physical Specifications | page 6-2 |
| Power Specifications | page 6-4 |
| Performance Specifications | page 6-5 |
| Media Module Specifications | page 6-7 |

# 6.1 Physical Specifications

## 6.1.1 Approvals

The switch has the following approvals:

**Table 6.2 -** ES-2810 Approvals

| Approval for | Standard |
|---|---|
| Safety | UL 1950,<br>CSA-C22.2 No. 950,<br>EN 60950 |
| Emission | FCC 47 CFR part 15 Class A,<br>EN 55022 Class A, |
| Susceptibility | EN 50082-1<br>IEC 1000-4-2<br>IEC 1000-4-3<br>IEC 1000-4-4<br>IEC 1000-4-5 |
| CE Mark | Yes |

## 6.1.2 Physical

The switch has the following physical specifications:

**Table 6.3 -** ES-2810 Physical Specifications

| Specification | Measurement |
|---|---|
| Dimensions | Width: 547 mm (21.5in.)<br>Height: 216mm (8.5in.)<br>Depth: 445mm (17.5in.) |
| Weight (approximate) | 8.6kg. (19lb.) |
| Recommended clearance | Sides: 100mm (4.0in.)<br>Rear: 190mm (7.7in.) |

## 6.1.3 Environmental

The switch has the following environmental specifications:

**Table 6.4 -** ES-2810 Environmental Specifications

| | |
|---|---|
| Operating temperature | +5 °C to +40 °C (+41 °F to +104 °F) |
| Storage temperature | –25 °C to +70 °C (–13 °F to +158 °F) |
| Humidity | Less than 85% non-condensing |
| Altitude | 3048 meters (10000 feet) |



## 6.1.4 LEDs

The switch has the following number of LEDs:

**Table 6.5 -** ES-2810 LEDs

| Status of | Number of LEDs |
|---|---|
| Port | 48 |
| Power | 1 |
| Status | 1 |
| Temperature | 1 |
| RPS | 1 |

## 6.1.5 Connections

The switch and modules have the following number of connections:

**Table 6.6 -** ES-2810 Connections

| Connections | Number |
|---|---|
| 10/100Mbps 10/100BaseTX (RJ-45) | 24 |
| CONSOLE port (DB-9) | 1 |

# 6.2 Power Specifications

## 6.2.1 Consumption

Power consumption: 100 W maximum

## 6.2.2 Power Supply

The power supply has:

**Table 6.7 -** ES-2810 Power Supply Specifications

| | |
|---|---|
| Nominal power supply voltages | 100-120 V AC, 2.5 A<br>200-240 V AC, 1.5 A<br>Autosensing<br>Class 1 protective ground |
| Frequency | 47 to 63 Hz |
| Main power connection | Detachable power cable |
| Input protection | Non-replaceable, internal fuse |

# 6.3 Performance Specifications

## 6.3.1 MAC addresses

The number of MAC addresses:

**Table 6.8 -** ES-2810 MAC Addresses

| MAC addresses per port | Number of ports available for multiple addresses |
|---|---|
| Max 8000 | All |



## 6.3.2 Switch Minimum Latency

11 microseconds at 100Mbps, and 30 microseconds at 10Mbps

## 6.3.3 Throughput

6.3 Gbps aggregate internal bandwidth

800 Mbps aggregate network bandwidth

## 6.3.4 CPU

IDT 79R3041 (16 MHz)

## 6.3.5 Memory Sizes

The memory sizes are as follows:

**Table 6.9 -** ES-2810 Memory

| Memory | ES-2810 Switch |
|---|---|
| Flash Memory (Mbytes) | 2 |
| DRAM (Mbytes) | 1 |
| Buffer RAM (Mbytes) | 4 |
| CPU RAM (Mbytes) | 1 |

## 6.3.6 Supported Protocols

This switch supports the following protocols:

**Table 6.10 -** ES-2810 Supported Protocols

| Subject | Document Reference |
|---|---|
| Bridge / Spanning Tree | IEEE 802.1D |
| Ethernet | IEEE 802.3 |
| Fast Ethernet | IEEE 802.3U |
| Auto-negotiation | IEEE 802.3X |
| UDP | RFCs 768, 950 and 1071 |
| TFTP | RFC 783 |
| IP | RFC 791 |
| ICMP | RFC 792 |
| TCP | RFC 793 |
| ARP | RFC 826 |
| Telnet | RFC 854 to 859 |
| BootP | RFCs 906, 951 and 1350 |
| RIP version 1 | RFCs 950 and 1058 |
| SMI | RFC 1155 |
| SNMP | RFC 1157 |
| MIB II | RFC 1213 |
| Ethernet-like MIB | RFC 1398 |
| Bridge MIB | RFC 1493 |
| Ether-like MIB | RFC 1643 |
| RIP version 2 | RFC 1723 |
| RMON | RFC 1757 |

# 6.4 Media Module Specifications

## 6.4.1 Range

There are two media modules for this switch:

**Table 6.11 -** ES-2810 Media Modules

| Media Module Name |
|---|
| 10/100TX Module FSM-4/TX |
| 100FX Module FSM-2/FX |



## 6.4.2 Physical

The media modules have the following physical specifications:

**Table 6.12 -** ES-2810 Media Module Physical Specifications

| | FSM-4/TX and FSM-2/FX |
|---|---|
| Dimensions | Width: 149mm (5.9in.)<br>Height: 37mm (1.5in.)<br>Depth: 238mm (9.4in.) |
| Weight (approximate) | 0.2kg. (0.45lb.) |

## 6.4.3 Connections

The media modules have the following number of ports and LEDs:

**Table 6.13 -** ES-2810 Media Module LEDS and Ports

| | FSM-4/TX | FSM-2/FX |
|---|---|---|
| 10/100Mbps 10/100Base-T (RJ-45) | 4 | — |
| 100Mbps 100Base-FX (SC) | — | 2 |
| Number of LEDs | 8 | 4 |

# CHAPTER 7 Troubleshooting

This chapter covers the topics listed in Table 7.1.

**Table 7.1 -** Topics in this Chapter

# 7.1 Troubleshooting Tools

The tools available for troubleshooting on the switch are:

**The LED Indicators** These are provided on the front panel of the switch. The LEDs indicate the overall switch status, and the status of each of the switch's ports and backplane segments (where applicable). See earlier in this manual for a full description of the LEDs and their use.

**SNMP** SNMP management in the switch is based on standard Management Information Base (MIB) II and Private Enterprise MIB extensions.

You can configure the switch to send SNMP Traps to defined locations, thus allowing the possibility of performing limited troubleshooting from an SNMP Management Center.

# 7.2 Troubleshooting Procedure

## 7.2.1 Isolating the Problem

If the switch has a problem for any reason, use the following procedure to isolate the problem:

1. Check the LEDs.

   The LEDs provide instant visual indication of the status of the switch and the status of each of its ports.

2. Check for any relevant messages in the Stack View Errors window.

   You may be asked to list this error message(s) by your supplier.

3. Check for any relevant messages in the Stack View System window.

   The System Log gives details about system events that occur during start-up and operation and also the general state of the switch. Typical information recorded in the System Log includes all major events during start-up, system changes, unexpected events and configuration errors. The System Log reports such things as software successfully located and loaded, ports enabled or disabled, and if any SNMP traps have been sent.

## 7.2.2 Further Evaluation of the Problem

If you still cannot resolve the problem satisfactorily from the information gained in the previous procedure, access the Monitor within Local Management. The Monitor is a valuable tool for the troubleshooting process and offers extensive information on the performance and the status of the switch hardware and software, the switch ports and the traffic patterns on each port.

The general facilities available within the Monitor are described in the following subsections. The use of these facilities depends on the problem and on any relevant information collected in the previous procedure.

# 7.3 Typical Problems and Causes

## 7.3.1 Typical Problems That Could Be Encountered

This section gives some examples of typical problems that could be encountered during the installation and configuration of the switch, and their possible cause. Configuration problems, defective cables and problems with communication among devices are the most common switch malfunctions.

## 7.3.2 Start-up Problems

**I've lost my password**

You are prompted for a password on the Login screen.

**Action:** Enter Maintenance Mode, and type: **`run defparm`**.

**Consequence:** This will reset the configuration to the default values.

**When I make changes to the switch's configuration, they take effect but as soon as the switch is powered off and on again the changes are lost**

When you change the switch's configuration, you are changing the current active configuration that is running in RAM. However, every time the switch starts-up it loads the configuration that is stored in its Flash Memory. Therefore, if you make a change to the configuration and want to keep it, you need to save the new configuration to the switch's Flash Memory.

**Action:** Save the configuration changes to Flash Memory.

To check the status of the configuration, select Configuration>Software.

**The switch is unable to start-up—I am using the network management center as the boot server**

If the switch cannot start from Flash Memory because, for example, the software in Flash Memory gets corrupted somehow, it issues BOOTP requests on the network to look for a boot server to provide the necessary software. This request contains the switch's MAC address, and any BOOTP server that has an entry in its bootptab file containing the switch's MAC address answers the request and downloads the bootptab information corresponding to the MAC address entry. However, because the network management center does not have a bootptab file in which to specify things like the filename of the software, this means that the switch cannot boot from the network management center in this way because the BootP requests issued from the switch do not contain any additional information, such as the boot software filename. Note that this is not a problem if you are using other boot servers that contain a bootptab file, and where you have written the name of the software in the bootptab.

**Action:** Enter Maintenance Mode and manually issue a BOOTP request including the filename; that is type the command: **`BootP <filename>`** at the prompt and the switch is then booted with the correct file from the boot server.

## 7.3.3 Performance Problems

**One or more workstations cannot communicate with a server or other device through the switch**

This symptom might be noticed on one or more segments connected to the switch, and could be caused by cable faults, inappropriate configuration or faulty installation.

**Action:** Check all connections and verify your configuration.

**The 100Mbps ports are not working, or work very poorly**

This is probably due to incorrect configuration of the auto-negotiation duplex settings and link speeds.

**Action:** Check the negotiated settings in the switch and compare them to the expected values.

**I have poor performance and high numbers of 2nd port drops**

There may be a loop in the network and Spanning Tree is not enabled.

**Action:** Either enable STP on all the ports (using **`Device Setup`**) or specific ports (using **`Port Setup`**).

## 7.3.4 Communication Problems

### 7.3.4.1 The Most Common Problems are Cable Problems

A high percentage of faults are caused by cable faults such as loose connections or inappropriately wired cables. Cable faults are easily remedied but can be awkward to track down, so you need a disciplined and methodical approach.

### 7.3.4.2 Spanning Tree Topology Changes

When a change is detected in the Spanning Tree network, the devices forming the Spanning Tree go into a learning state to determine the optimal routes between network segments. During this learning state, the switch will not forward data traffic.

This is a normal occurrence for Spanning tree devices and no remedial action is required. However, if the switch goes into the learning state too frequently, the Spanning Tree maybe unstable and should be examined and possibly reconfigured.

### 7.3.4.3 To Troubleshoot Communications Problems

If the POWER LED and the STATUS LED are both on, but one or more of the port STATUS LEDs are off, then:

1. Reset the switch using the **Reset** button.
2. Check the STATUS LED for each switch port to which a cable is attached.

### 7.3.4.4 VLANs

The use of VLAN policies can lead to unexpected communication problems. If the policies are not designed with care or ports are not able to reach network services, check your VLAN policies and use the VLAN monitoring to review the VLAN membership for that port or address.

# 7.4 Contacting the Technical Assistance Center (TAC)

## 7.4.1 Introduction

If you are unable to solve the problem and want to report the problem to FORE Systems Technical Assistance Center (TAC), there are certain things that you can do to enable us to begin solving your problem quickly. Stack View makes the gathering of such information easy, and presents it in an easy-to-interpret format.

## 7.4.2 Things to do Prior to Contacting TAC

To ensure that your problem gets treated as efficiently as possible right from the start, TFTP a report and parameter block from the switch. If it is not possible to TFTP from the switch, try to obtain the product number and the software ID and version number, any error messages in the Error and System Logs, and a copy of the switch's configuration.

The following information must always be supplied when contacting Customer Support for help:

1. The scope and characteristics of the problem. How severe is the problem? Is the switch dead? Are any of the ports malfunctioning? If so, which ports? Is the whole network down?
2. A quick sketch of your configuration.
3. Is the problem reproducible? If yes, how?
4. Is it a new installation, or has it been running for a while?
5. When was the last time it was working correctly? What has happened since then that might have affected the switch?

The information in this report can be of great help to us in finding a solution to the problem as quickly as possible.

## 7.4.3 Further Information on TAC

For information about FORE's support service, refer to "Technical Support" on page ii of the Preface.

# APPENDIX A Concepts in Switching

This chapter gives a introduction to the concepts behind the features in the switch:

- Forwarding Mode

  Each port can operate in adaptive, cut-through, fragment-free or store-and-forward forwarding mode. A description of each of the forwarding modes and when to configure them is given in “Forwarding Modes” on page A-2.
- Flow Control
- You can select half- or full-duplex for each port. This is described in “Half- and Full-duplex” on page A-8.
- Auto-negotiation
- Port Filters
- Internet Protocol
- Give the switch an IP address for use in SNMP and TFTP. For details see “IP Addresses” on page A-16.
- Spanning Tree
- Configure the Spanning Tree priorities and costs associated with use of the switch and ports. For details see “Spanning Tree” on page A-20.
- Permanent MAC addresses
- Virtual LANs (VLANs)

# A.1 Forwarding Modes

## A.1.1 Forwarding Mode Affect on Latency

Latency is the delay measured from the time the packet first enters a network device until it leaves it. The closer a device is to zero latency, the better.

The type of network can affect latency. Over wide area networks, latency is negligible in comparison to the time it takes the signals to travel over long distance lines. On local area networks, reducing latency normally increases performance.

Unfortunately, reducing the latency can often lead to an increase in errors on the network. The ideal situation is

Change the forwarding modes to provide added reliability and flexibility. For example, if you are concerned about the generation of errors on a network, you can configure the ports to store-and-forward mode to ensure safe transfer of data.

## A.1.2 Possible Forwarding Modes

You can specify one of four possible forwarding modes you can specify for each port:

- Cut-through
- Fragment-free
- Store-and-forward
- Adaptive

## A.1.3 Forwarding Policy

If two communicating ports (receive port and transmit port) have different forwarding modes, then they use the “safest” mode. For example, if one port is configured for fragment-free and the other port is configured for store-and-forward, then traffic between the two ports in either direction is always switched using store-and-forward.

## A.1.4 CRC Errors

Cyclic Redundancy Check (CRC) errors are the sum of Frame Check Sequences, longs, very longs, alignment errors and jabbers.

## A.1.5 Fragment

A fragment is a frame consisting of only part of a packet; these can be caused by collisions on the network and are normal occurrences.

## A.1.6 Cut-through Forwarding

Cut-through forwarding sends the packet to the destination as soon as the first 14 bytes of the packet are read—an approximate latency of 30 microseconds for 10Mbps devices and 11 microseconds for 100Mbps devices. The delay is minimal and the packets reach their destination in the shortest possible time.

The packets are sent through the switch as a continuous flow of data—the transmit and receive rates are always the same. Because of this, cut-through forwarding cannot pass packets to higher speed networks, for example, to forward packets from a 10Mbps to a 100 Mbps Ethernet network.

Since the switch has forwarded most of the packet when the CRC is read, the switch cannot discard packets with CRC errors. However, the CRC check is still made and, if errors are found, the error count is updated.

Cut-through forwarding is recommended for networks intended to provide one switch port per user, or for lightly loaded networks. It is essential for multimedia applications and ideal for workgroup environments where minimum delays are required.

## A.1.7 Fragment-free Forwarding

Fragment-free forwarding is suitable for backbone applications in a congested network, or when connections are allocated to a number of users.

Fragment-free forwarding checks that there are no collisions within the first 64 bytes of the packet—the minimum valid message size required by the IEEE 802.3 specification. This guarantees that message fragments less than 64 bytes (runts) are not forwarded to other network segments. Runts are typically the result of collision fragments.

The packets are sent through the switch as a continuous flow of data—the transmit and receive rates are always the same. Because of this, fragment-free forwarding cannot pass packets to higher speed networks, for example, to forward packets from a 10Mbps to a 100 Mbps Ethernet network. Therefore, if you opt for fragment-free forwarding, you cannot make direct connections to higher speed networks (like FDDI) from that port.

Fragment-free forwarding offers a compromise between cut-through (which offers the fastest possible forwarding at the expense of error checking) and store-and-forward (which offers maximum error checking at the expense of forwarding speed), to provide a latency of approximately 60 microseconds and sufficient error checking to eliminate the most common errors.

## A.1.8 Store-and-forward Forwarding

Store-and-forward forwarding temporarily stores a packet and checks it against the CRC field. If the packet is error free, it is forwarded; otherwise, it is discarded.

Store-and-forward forwarding is therefore the best forwarding mode to prevent errors being forwarded throughout the network. The buffering used by store-and-forward also allows the switch to dispatch packets at a different rate than it receives them—for example, to forward packets from a 10Mbps network to higher speed networks such as a 100Mbps Ethernet.

## A.1.9 Adaptive Forwarding

Adaptive forwarding mode is a user-defined facility to maximize the efficiency of the switch. Adaptive forwarding starts in the default switch forwarding mode you have selected in the `Switch & Port` window (cut-through if you selected adaptive mode as the default forwarding mode). Depending on the number of runts and CRC errors at that port, the mode changes to the "best" of the other two forwarding modes. As the numbers of runts and CRC errors change, so does the forwarding mode. This is best illustrated by:

**Table A.1 -** Adaptive Forwarding Modes

| Forwarding mode: | Detects: | Then, adaptive mode changes the forwarding mode to: |
|---|---|---|
| Cut-through | High numbers of CRC errors | Store-and-forward |
| | High numbers of runts | Fragment-free |
| Fragment-free | High numbers of CRC errors | Store-and-forward |
| | Low numbers of runts | Cut-through |
| Store-and-forward | Low numbers of CRC errors | Fragment-free |
| | Low numbers of CRC errors and runts | Cut-through |


While CRC errors and runts are the most likely parameters to cause the forwarding mode to change, they are not the only ones.

## A.1.10 Latency

Delays depend on the forwarding mode:

**Table A.2 -** Latency Periods for Forwarding Modes

| | Cut-through | Fragment-free | Store-and-forward |
|---|---|---|---|
| Min. Latency (in microsec.) | Low (10 Mbit is < 30 100 Mbit is < 11) | Medium (< 60) | High (Depends on packet size) |
| Amount of packet read | 14 bytes: Destination address + Source address + Type / Length field) | 64 bytes (IEEE 802.3) | All (CRC) |
| Error detection | None | Runts | All |
| Suitable for | One user per port. Light loads. Applications requiring low latency forwarding. | Many users on one connection. Congested networks. | Communication with higher-speed networks. A port with many errors. |

# A.2 Flow Control

## A.2.1 Flow Control Concept

The switch can become overloaded if incoming frames arrive faster than the switch can process them, and this results in the frames being discarded until the overload condition passes. The flow control mechanism overcomes this problem and eliminates the risk of lost frames.

If a potential overload situation occurs, the switch simply generates a “pseudo collision” which forces all transmitting stations to immediately stop transmitting and wait a random amount of time before trying to retransmit. Followi7ng a simulated collision, any buffered frames are sent to their destination—clearing the switch’s buffers and allowing it to receive future frames.

## A.2.2 When to Use Flow Control

The flow control mechanism is ideal for situations where only one station is attached to one switch port—do not use flow control on a port connected to a hub. However, consider the case where there is more than one station attached to a port as shown below:

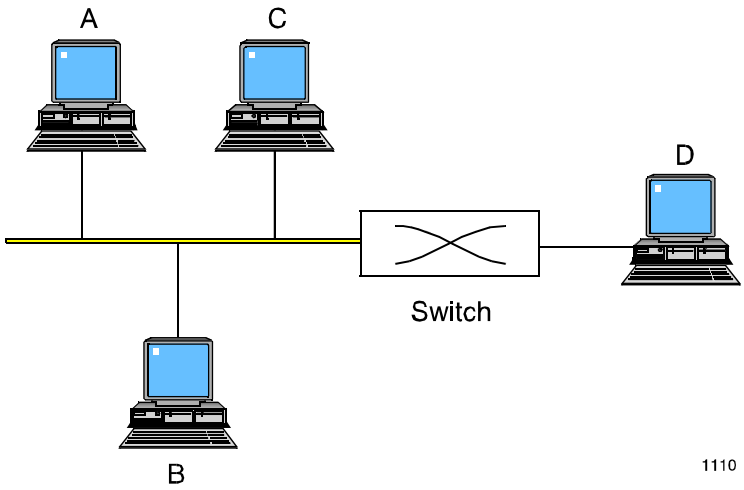



**Figure A.1 -** Flow Control

If station C tries to send data to station D via the overloaded switch, station C is "invited" to stop transmitting and wait a random time before trying again. Because stations A and B are on the same cable segment as station C, they also detect the collision and are therefore also prevented from sending data to each other (not just to station D), for as long as the switch is overloaded.

Flow control influences all ports that have flow control enabled—regardless of which port(s) is responsible for the overload situation.

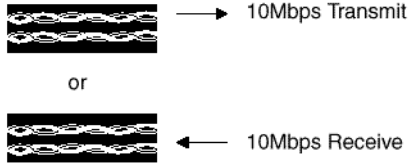
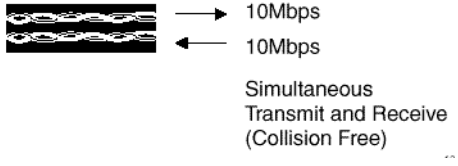
# A.3 Half- and Full-duplex

## A.3.1 Half-duplex and Full-duplex Concepts

Half-duplex works optimally only if one device is transmitting and all the other devices are receiving—otherwise, collisions occur. When the collisions are detected, the devices causing the collision wait for a random time before retransmitting. This means that at half duplex, Ethernet throughput is limited by the need to retransmit data when collisions occur. Half-duplex is the most common transmission method and is adequate for normal workstation and PC connections.

Full-duplex provides dual communication on a point-to-point connection and allows each device to simultaneously transmit and receive on a connection. Full-duplex mode is typically used to connect to other switches or to connect fast access devices such as workgroup servers.

**Table A.3 -** Half-duplex and Full-duplex

| Transmission mode | | Capacity |
|---|---|---|
| Half-duplex |  | Less than 10Mbps when communicating |
| Full-duplex |  | 20 Mbps |

NOTE

To use full-duplex communication, both ends of the connection must be configured to operate in full-duplex mode, and the connecting device must have a full-duplex adapter installed. Full-duplex operation is only possible on point-to-point Ethernet connections that use separate conductors or fibers for transmit and receive, such as 10Base-T and 100Base-FX cabling. Full-duplex operation is not possible on connections using coaxial or AUI (10Base-5) cables or with most hubs.

## A.3.2 When to Use Full-duplex

Some servers perform better using full-duplex because they simultaneously handle traffic from many clients: some are transmitting data to the server, while others are receiving data from the server. Switch-to-switch connections certainly benefit from full-duplex transmission.

Individual workstations normally run applications traditionally written for half-duplex, request/response network connections, and are unlikely to benefit from being configured as full-duplex. For example, the application may request a service on a server and then wait for a reply before continuing operations. In this case, if the server connection was full-duplex, the server might respond to the request while simultaneously receiving from another station; a full-duplex connection for the workstation would typically offer no advantage.

## A.3.3 Auto Duplex

Auto duplex negotiates whether the attached device is transmitting in half- or full-duplex, and then automatically changes that port to that mode.

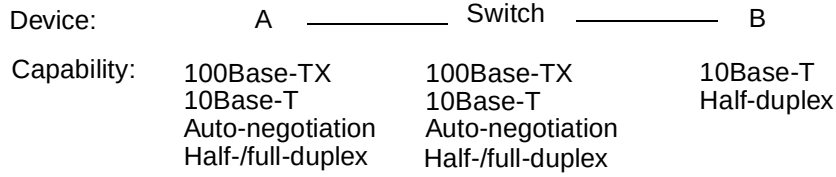
# A.4 Auto-negotiation

## A.4.1 Auto-negotiation Concept

Auto-negotiation follows the IEEE 802.3u 100Base-T specification to improve the effectiveness of dual speed links (such as the base ports and the 10/100TX Media Module). They have the capability to work at either of their speeds (10Mbps or 100Mbps) and either of the duplex modes (half- or full-duplex).

Normally you would need to configure the port on the switch with a specific speed or duplex mode, but that is not required with auto-negotiation — it detects the capabilities of the other devices (over a common link) and configures itself to use the same technology automatically; this gives maximum efficiency.

To illustrate how auto-negotiation works, imagine two devices connected via a switch as shown in the figure below.




Auto-negotiation allows the Switch port to select the best transmission speed and duplex mode—based on the capabilities of the device at the other end.

The link between Device A and the Switch has Auto-negotiation enabled at both ends. Since both ends support 100Mbps full-duplex mode, this mode is selected.

Device B is also connected to the Switch, but only supports 10Mbps half-duplex transmission. The Switch automatically detects this and select 10Mbps half-duplex transmission for this port.

## A.4.2 Checklist for Problems

If you have problems with auto-negotiation, here are some helpful hints:

- If there is no link pulse:
  - Check the cable
  - Check auto-negotiation setup
  - A match must exist between the stations
- If the port is disabled:
  - Check that the configuration of the port is correct
  - Check that the modes you have entered match
  - For example, Speed is used during auto-negotiation

# A.5 Port Filters

## A.5.1 Introduction

It is possible to increase network security by using port filters. Adding a filter to a port determines where data can come from (using port numbers and MAC addresses) and go to (using port numbers and MAC addresses) on the network. This means that you can have a high level of network security.

## A.5.2 Purpose

The Port / MAC Filter facility lets you:

- Specify which ports the MAC address can be learned on
- Specify which ports the MAC address can send packets to
- Specify which ports can receive Multicast packets
- Send packets from one port to other specified ports
- Change the information on an existing port or MAC address
- Delete filtering on an existing port or MAC address
- Enable or disable the filtering system
- Scan the specifications you have made to detect any trivial errors

## A.5.3 Conflicts with Other Settings

When you add or make changes to Port / MAC filter settings, it is possible it may conflict with VLANs or permanent MAC address settings in other windows of the switch. To reduce the danger of altering the switch configuration by mistake, certain priorities have been made. These are listed in “Port Filter Priorities” on page A-15.

## A.5.4 Add a Port Filter

### A.5.4.1 Introduction

You can add up to 100 filters. When you add a filter, you choose from the ports available at that time. If more ports are added later (for example, by connecting an expansion module), you should edit your filters to include the new ports.

When you remove ports (for example, disconnecting the expansion module), those ports are removed from the filter set-up. If these ports are the only ones in the source or destination port list, the filter is deleted.

If you choose all the ports available, the screen shows `All` in the list. If you then connect an expansion module—thus adding ports that are not in that filter—the ports are listed individually.

To show that a source port is not required for the filter, "--" is used in the `Source ports` list.

### A.5.4.2 Types of Port Filter Entry

There are three types of port filter entry:

- Port relation
- MAC unicast
- MAC multicast

## A.5.5 MAC addresses

### A.5.5.1 Entering a MAC Address

There are limited options when entering a MAC address:

**Table A.4 -** MAC Address Options

| Enter | Possible? | Explanation |
|---|---|---|
| Broadcast address (FFFFFFFFFFFF) | No | This address must be available to all ports. |
| STP Multicast (0180C2000000) | No | This multicast is used for switch functions. |
| Limit flooding of Multicast addresses to certain ports | Yes | Create a filter (for the corresponding Multicast address) with destination ports specified. The multicast is only transmitted to these ports on the switch. |
| Multicast kept within existing VLAN | Yes | VLAN constraints. |

### A.5.5.2 Violation of Port/MAC Filter

If a MAC address violates the Port/MAC filter setting, an error message shows the offending MAC address and the port on which the violation occurred. An SNMP trap containing the port number is also sent on the network.

### A.5.5.3 The Switch's Own MAC Address is Part of a Filter Entry

This entry is ignored by the filter and an entry in the error log indicates what happened.

## A.5.6 Port Filter Priorities

### A.5.6.1 Introduction

When you make changes to VLANs or permanent MAC addresses in other windows of the switch, it is possible you may have conflict between the Port/MAC filter settings and other settings. To reduce the danger of altering the switch configuration by mistake, certain priorities have been made.

### A.5.6.2 VLANs

A port VLAN always has priority over a Port/MAC filter setup. When you add or change a filter setup, you can only specify ports that belong to the same VLAN; this ensures the packets never go beyond the limits of that VLAN.

### A.5.6.3 Permanent Port Entries

A permanent MAC address on a port always has priority over a Port/MAC filter setup. When you add or change a filter setup, you can only specify the port that is the permanent MAC address.

### A.5.6.4 To Remove Conflicting Setups

When you change to a VLAN or permanent MAC address entry, the switch automatically checks for configuration conflicts with the Port/MAC filters. If a conflict exists, you have two options:

- Change the VLAN or permanent MAC address setup:

  This removes the conflict between the setups
- Keep the VLAN or permanent MAC address setup:
- This automatically disables the Port/MAC filtering

If the Port/MAC filtering is disabled, you cannot use the Port/MAC filtering facility until all the conflicting settings have been changed in the Port/MAC filter, VLAN or permanent MAC address entry.

### A.5.6.5 Port–port Relationships Versus Standard MAC Entries

A port relationship takes priority over a regular MAC entry. A filter for a standard MAC address can only accept destination ports that are a subset of the port–port relationship entry.

# A.6 IP (Internet Protocol)

The switch uses IP for management. You need to configure the switch's IP parameters if:

- The switch is to be configured / managed over the network from a boot server or network management system
- You want to use SNMP management
- You want to be able to establish a TELNET session to Local Management over the network

## A.6.1 IP Addresses

### A.6.1.1 Address Assignment

An IP address consists of two parts: network and host (or local) address. The network part must be globally unique and is assigned by InterNIC (International Network Information Center). The host address is the responsibility of the network manager.

In private networks, where connections to other IP networks are not available, locally assigned IP addresses can be used.

### A.6.1.2 Frame Types and Type Codes

The following Ethernet type codes are used in the IP environment:

**Table A.5 -** Frame Types and Codes

| Type field | Description |
|---|---|
| 0800 | DOD Internet Protocol (IP) |
| 0806 | Address Resolution Protocol |

## A.6.1.3 IP Address Structure

### A.6.1.3.1 Address Notation

IP addresses are 32-bit numbers. The most common notation for IP addresses divides the 32-bit address into four 8-bit fields and specifies the value of each field as a decimal number (from 0 to 255, each representing an 8-bit octet). Each number field is separated by a period (for example, 14.0.65.3). This is called the dotted decimal notation.

### A.6.1.3.2 Network Numbers

The 32-bit address field consists of a network and a local host part. They are divided into different address classes which differ in the number of bits allocated to the network part and the host part (local address) of the address. The value of the first octet in the IP address defines the address class (classes A, B, C, D).

### A.6.1.3.3 Class A Address

The class A address comprises a 7-bit network number and a 24-bit host address. The highest order bit is set to 0. This allows 126 class A networks.

**Table A.6 -** Class A Addresses

| 1 | | | | | | | | 2 | | | | | | | | 3 | | | | | | | | 4 | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| 0 | Network | | | | | | | Host Address | | | | | | | | | | | | | | | | | | | | | | | |

### A.6.1.3.4 Class B Address

The class B address comprises a 14-bit network number and a 16-bit host address. The two highest-order bits are set to 1 0. This allows 16256 class B networks.

**Table A.7 -** Class B Addresses

| 1 | | | | | | | | 2 | | | | | | | | 3 | | | | | | | | 4 | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| 10 | Network | | | | | | | | | | | | | | | Host Address | | | | | | | | | | | | | | | |

### A.6.1.3.5 Class C Address

The class C address comprises a 21-bit network number and a 8-bit host address. The three highest-order bits are set to `1 1 0`. This allows 2072640 class C networks.

**Table A.8 -** Class C Addresses

| 1 | | | | | | | | 2 | | | | | | | | 3 | | | | | | | | 4 | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| 1 1 0 | | | Network | | | | | | | | | | | | | | | | | | | | | Host Address | | | | | | | |

### A.6.1.3.6 Class D Address

The class D address is used as a multicast address. The four highest-order bits are set to `1 1 1 0`.

**Table A.9 -** Class D Addresses

| 1 | | | | | | | | 2 | | | | | | | | 3 | | | | | | | | 4 | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| 1 1 1 0 | | | | Multicast Address | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**NOTE**

No addresses are allowed which have the four highest-order bits set to 1 1 1 1 (also known as class E address).

### A.6.1.3.7 Addresses Available

The following IP addresses are available for the different IP address classes:

NOTE

n = network part of the address,
h = host part of the address.

**Table A.10 -** Address Ranges by Class

| Class | Address Range available | Notation |
|---|---|---|
| A | 1.0.0.0 through 126.0.0.0<br>(127.h.h.h reserved) | n.h.h.h |
| B | 128.0.0.0 through 191.254.0.0 | n.n.h.h |
| C | 192.0.0.0 through 223.255.254.0 | n.n.n.h |
| D | 224.0.0.0 through 239.255.255.255 for multicasts. | n.n.n.n |
| E | 240.0.0.0 through 247.255.255.255 reserved. | n.n.n.n |

### A.6.1.3.8 IP Address Class Overview

The table below summarizes the different classes of IP address:

**Table A.11 -**

| | Class A | Class B | Class C |
|---|---|---|---|
| Max. no. of networks | 127 | 16256 | 2072640 |
| Max. no. of computers per network | 16777214 | 65534 | 254 |
| Network no. part | First field | First two fields | First three fields |
| Network no. range | 001 to 127 | 128 000 to<br>191 255 | 192 000 000 to<br>223 255 255 |
| Host no. part | Last three fields | Last two fields | Last field |
| Host no. range | 000 000 001 to<br>255 255 254 | 001 001 to<br>255 254 | 001 to 254 |

# A.7 Spanning Tree

You can change the:

- Priority given to the switch
- Maximum length of time information is retained by the switch
- Time between transmitted Configuration BPDUs
- Time the switch spends in the Listening and Learning states

## A.7.1 Warning When Using VLANs

It is important to be aware of problems that may arise when using Spanning Tree and VLANs. The Spanning Tree can use alternative paths (such as different ports) to get messages to their destination. VLANs specify which ports can receive messages.

***WARNING!***

When using the Spanning Tree facility, only use one VLAN. Using two or more VLANs may cause unexpected alterations in your network topology.

## A.7.2 Spanning Tree Protocol

### A.7.2.1 Spanning Tree Protocol Concept

Since alternative paths are desirable for backup and other purposes, IEEE and ISO have proposed a standard to solve the problem of "network loops". The solution is called "The Spanning Tree Protocol", and is described in IEEE document 802.1D, "Local MAC Bridges".

### A.7.2.2 Bridging Loops

Within the Spanning Tree Algorithm, switches connected in a LAN must detect potential "bridge loops", and then remove these loops by blocking the appropriate ports to other switches. This is illustrated in the following diagram:

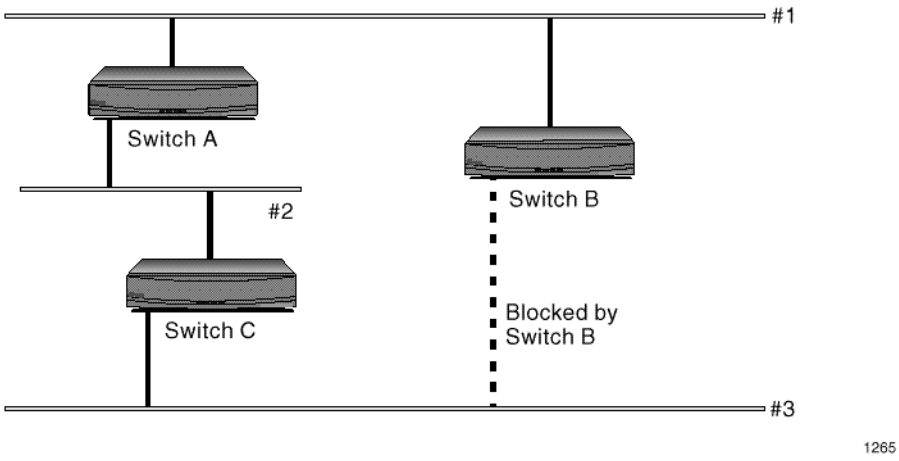



**Figure A.2 -** Spanning Tree and Bridge Loops

An alternate path has been established by connecting Switch B in parallel with Switches A and C — this also creates a potential bridge loop. However, by using the Spanning Tree Algorithm, Switch B breaks the loop and blocks its path to segment 3.

### A.7.2.3 Bridge Failure

If Switch A fails, the Spanning Tree Algorithm must be capable of activating an alternative path, such as Switch B.

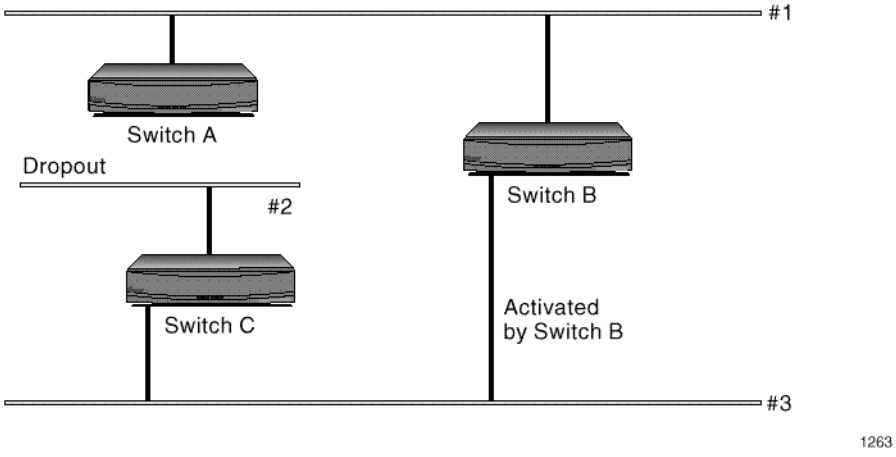



**Figure A.3 -** Spanning Tree and Bridge Failures

### A.7.2.4 Network Extension

If the network is extended by adding Switch D, the Spanning Tree Algorithm must be capable of adapting automatically to the new topology, that is Switch B stops looping by blocking the path to segment 3.

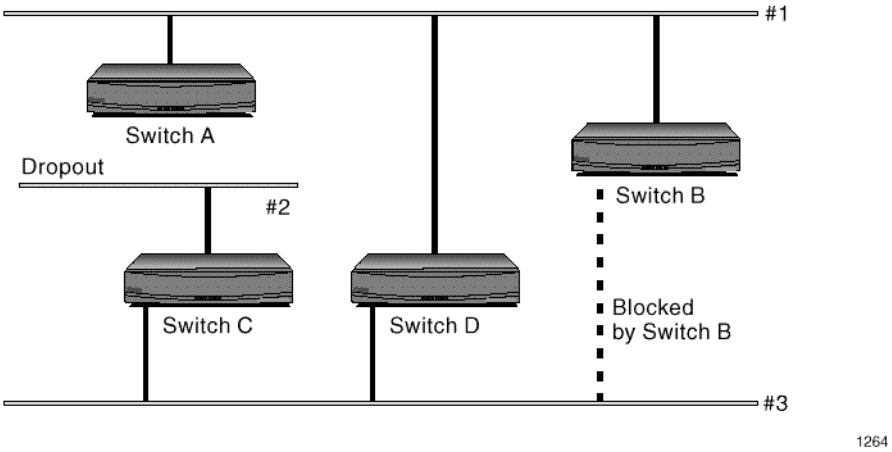



**Figure A.4 -** Spanning Tree Adapting to New Topology

### A.7.2.5 Port States When Enabled

Each switch is identified by a switch ID, and each port (interface) on a switch is identified by a Port ID.

Ports can be either disabled or enabled. Ports which are enabled can be in one of the following states:

**Listening** Switches send messages to one another to establish the network topology and the optimal paths to the different segments of the network. Other data is not transmitted.

**Blocking** The switch enters the Blocking State if a path with higher priority is found to exist during the Listening State. Normal data is not transmitted.

**Learning** The switch enters the Learning State if no path with a higher priority is found during the Listening State. Learned entries are entered in the Unicast Destination Forwarding Table. Normal data is not transmitted.

**Forwarding** The switch enters the Forwarding State after having been in the Learning State for a predefined time period. Normal data is transmitted.

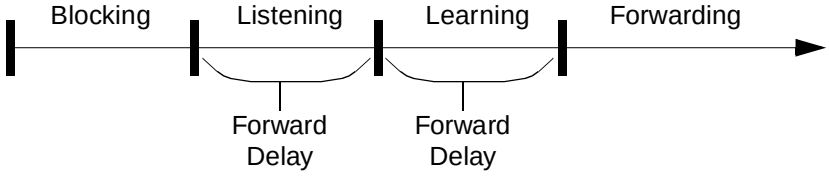



**Figure A.5 -** Port States

### A.7.2.6 Disabled Ports

Ports which are disabled do not adapt to solve the problem network loops using the Spanning Tree Protocol.

### A.7.2.7 Spanning Tree Topology

The cost factor is used to calculate the distance from each port of a switch to the Root Switch. On the basis of this, each port on a switch is assigned one of the following states:

**Root Port** The port that is closest to the Root Switch. Only one port on each switch is assigned as the Root Port.

**Designated Port** The ports that connect to switches further away from the Root Switch than the switch. The Root Switch only has Designated Ports.

**Blocking** If any ports are not assigned a Root Port or a Designated Port State, they are assigned a "Blocking" State. Frames (with the exception of Configuration BPDUs) are not accepted or transmitted by the port when it is in the Blocking State. The port can be said to be in stand-by.

### A.7.2.8 Frame Propagation

By enforcing this strict hierarchy and by only forwarding frames between Root Ports and Designated Ports, the possibility of bridging loops is removed.

Frames cannot be sent directly between switches (except via the Root Switch).

### A.7.2.9 7-hop Limit

In addition to the strict bridging hierarchy imposed by the Spanning Tree Algorithm, a 7-hop limit is introduced. Frames should not pass more than 7 bridges and this limits the size of the bridged network.

### A.7.2.10 Configuration BPDU Messages

To establish the stable paths, each switch sends Configuration BPDU Frames to its neighboring switches. These Configuration BPDU messages contain information about the spanning tree topology. The contents of these frames only changes when the bridged network topology changes or has not been established.

### A.7.2.11 Configuration BPDU Message Propagation

When a bridged network is in a stable condition, switches continue to send Configuration BPDU Frames to its neighboring switches at regular intervals. Configuration BPDU Frames are transmitted down the spanning tree from Designated Ports to Root Ports. If a Configuration BPDU is not received by the Root Port on a switch in a predefined time interval (for example, because a switch along the path has dropped out), the port enters the Listening State to redetermine its stable path.

### A.7.2.12 MAC Address Ageing

MAC address ageing is overruled by changes in the Spanning Tree. When the Spanning Tree is bridging and blocking, the topology of the network can change. This means the MAC addresses are changing and the Spanning Tree overrides the set MAC address ageing value.

# A.8 Permanent Address Assignments

You can:

- See which ports have MAC addresses permanently attached to them
- Specify if other addresses are allowed to use individual ports
- Specify a permanent (locked) MAC address for each port
- Delete user addresses from the port list

## A.8.1 Permanent Explanation

### A.8.1.1 Address Table

The switch learns the topology of the network by matching the address of the station (which sent the incoming frame) to the port on which it arrived. In this way it compiles an address table of which stations are connected to each port.

Once an address is learned, a frame destined for that address is forwarded only on the port to which it is attached. The switch removes "old" entries from the table to ensure that the address table is always kept up-to-date.

### A.8.1.2 Permanent Address

You can make stations permanent on a port so that they are never removed from the switch's address table regardless of how long they have been quiet.

Print servers are a good example of silent network devices — they are not able to send packets to the switch and the MAC address is never learned by the switch.

### A.8.1.3 Why Make Addresses Permanent?

If the switch receives a frame with an unknown destination address, it sends (or "floods") the frame out on all ports. You can reduce flooding by specifying permanent addresses on a port; these addresses are not removed regardless of how long they have been quiet.

You can allow only the defined MAC address(es) for a port to be able to use that port, thus increasing security by preventing the intrusion of unknown devices.

Unfortunately, defining permanent addresses on the ports can reduce your network's ability to move stations from one port location to another.

# A.9 VLANs (Virtual LANs)

The use of VLANs lets you:

- Create separate user groups
- Easily relocate people (and their PCs) within the building
- Limit broadcast and multicast traffic
- Increase security because the groups can not communicate with each other

## A.9.1 Policy-based VLAN

These VLANs can be created based on the following policies:

- Ports
- IP addresses
- IP subnets
- MAC addresses
- Any combination of the four policies above

## A.9.2 Warning When Using VLANs

It is important to be aware of problems that may arise when using Spanning Tree and VLANs. The Spanning Tree can use alternative paths (such as different ports) to get messages to their destination. VLANs specify which ports can receive messages.

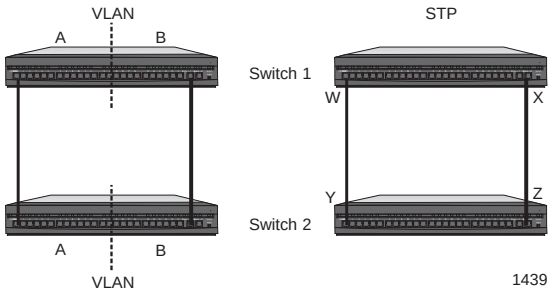



**Figure A.6 -** Spanning Tree and VLANs

In the above diagram, we have two switches. To the left, we see the two switches connected and the ports are grouped in two VLANs: A and B. On the right, we have enabled STP; STP blocks the path between X and Z (to avoid looping) and, therefore, destroys the VLAN setup (because the VLAN needs these ports to receive messages).

## A.9.3 VLAN Explanation

You can create separate VLANs by assigning port numbers of the switch, IP addresses of devices, IP subnets and MAC addresses to a VLAN on the switch. This effectively "cuts" the switch into completely independent segments. VLANs are useful for:

- Security issues. Groups can be isolated and the group traffic can be prevented from being switched to other groups.
- Limiting Broadcast and Multicast traffic on the network to the specific VLAN.
- Resource allocation (departmental vs. common resources). Certain groups can be allocated to specific resources, such as servers.
- Application specific reasons, for example to provide firewall protection.

If you have a network that is subnetted, you can configure the switch's VLANs to match the number of subnets you have created. You can then use routers to connect the subnets and provide filtering and firewall protection.

### A.9.3.1 Membership of VLANs

It is important to note that a device can be a member of more than one VLAN. Any conflict in membership between the VLANs can be checked using Stack View.

### A.9.3.2 Designated Management VLAN

On the switch, there is always one VLAN that is designated to manage via SNMP. This VLAN cannot be deleted unless another is selected as the Designated Management VLAN.

### A.9.3.3 IP Learning

There are some ports you will only want to use the IP policy — not port or MAC address policies. This is called IP learning, and to ensure this happens the port can be selected to support IP learning.

# Glossary

**802.1d Spanning Tree Bridging** - the IEEE standard for bridging; a MAC layer standard for transparently connecting two or more LANs (often called subnetworks) that are running the same protocols and cabling. This arrangement creates an extended network, in which any two workstations on the linked LANs can share data.

**802.3 Ethernet** - the IEEE standard for Ethernet; a physical-layer standard that uses the CSMA/CD access method on a bus-topology LAN.

**802.5 Token Ring** - the IEEE physical-layer standard that uses the token-passing access method on a ring-topology LAN.

**AAL (ATM Adaptation Layer)** - the AAL divides the user information into segments suitable for packaging into a series of ATM cells. There are several types of AALs in use. FORE Systems currently supports AAL 5 and AAL 3/4. AAL 3/4 supports connection-oriented VBR data transfer and connectionless VBR data transfer, respectively. AAL 5 is defined as Simple and Efficient Adaptation Layer (SEAL).

**AAL Connection** - an association established by the AAL between two or more next higher layer entities.

**ABR (Available Bit Rate)** - a type of traffic for which the ATM network attempts to meet that traffic's bandwidth requirements. It does not guarantee a specific amount of bandwidth and the end station must retransmit any information that did not reach the far end.

**ACR (Allowable Cell Rate)** - parameter defined by the ATM Forum for ATM traffic management. ACR varies between the MCR and the PCR, and is dynamically controlled using congestion control mechanisms.

**Address Mask** - a bit mask used to identify which bits in an address (usually an IP address) are network significant, subnet significant, and host significant portions of the complete address. This mask is also known as the subnet mask because the subnetwork portion of the address can be determined by comparing the binary version of the mask to an IP address in that subnet. The mask holds the same number of bits as the protocol address it references.

**Agent (SNMP)** - a component of network- and desktop-management software, such as SNMP, that gathers information from MIBs.

**AIS (Alarm Indication Signal)** - a line AIS is asserted when a 111 binary pattern is detected in bits 6, 7, 8 of the K2 byte for five consecutive frames. A line AIS is removed when any pattern other than 111 is detected in these bits for five consecutive frames.

**alarm** - an unsolicited message from a device, typically indicating a problem with the system that requires attention.

**AMI (ATM Management Interface)** - the user interface to FORE Systems' *ForeThought* switch control software (SCS). AMI lets users monitor and change various operating configurations of FORE Systems switches and network module hardware and software, IP connectivity, and SNMP network management.

**ANSI (American National Standards Institute)** - a private organization that coordinates the setting and approval of some U.S. standards. It also represents the United States to the International Standards Organization.

**API (Application Program Interface)** - a language format that defines how a program can be made to interact with another program, service, or other software; it allows users to develop custom interfaces with FORE products.

**APP (application program)** - a complete, self-contained program that performs a specific function directly for the user.

**AppleTalk** - a networking protocol developed by Apple Computer for communication between Apple's products and other computers. Independent of the network layer, AppleTalk runs on LocalTalk, EtherTalk and TokenTalk.

**ARP (Address Resolution Protocol)** - a method used to resolve higher level protocol addressing (such as IP) into the appropriate header data required for ATM; i.e., port, VPI, and VCI; also defines the AAL type to be used.

**ASCII (American Standard Code for Information Interchange)** - a standard character set that (typically) assigns a 7-bit sequence to each letter, number, and selected control characters.

**Assigned Cell** - a cell that provides a service to an upper layer entity or ATM Layer Management entity (ATMM-entity).

**asxmon** - a FORE program that repeatedly displays the state of the switch and of all its active ports.

**ATDM (Asynchronous Time Division Multiplexing)** - a method of sending information that resembles normal TDM, except that time slots are allocated as needed rather than preassigned to specific transmitters.

**ATM (Asynchronous Transfer Mode)** - a transfer mode in which the information is organized into cells. It is asynchronous in the sense that the recurrence of cells containing information from an individual user is not necessarily periodic.

**ATM Forum** - an international non-profit organization formed with the objective of accelerating the use of ATM products and services through a rapid convergence of interoperability specifications. In addition, the Forum promotes industry cooperation and awareness.

**ATM Layer link** - a section of an ATM Layer connection between two adjacent active ATM Layer entities (ATM-entities).

**ATM Link** - a virtual path link (VPL) or a virtual channel link (VCL).

**ATM Peer-to-Peer Connection** - a virtual channel connection (VCC) or a virtual path connection (VPC) directly established, such as workstation-to-workstation. This setup is not commonly used in networks.

**ATM Traffic Descriptor** - a generic list of parameters that can be used to capture the intrinsic traffic characteristics of a requested ATM connection.

**ATM User-to-User Connection** - an association established by the ATM Layer to support communication between two or more ATM service users (i.e., between two or more next higher layer entities or between two or more ATM entities). The communication over an ATM Layer connection may be either bidirectional or unidirectional. The same Virtual Channel Identifier (VCI) is used for both directions of a connection at an interface.

**atmarp** - a FORE program that shows and manipulates ATM ARP entries maintained by the given device driver. This is also used to establish PVC connections.

**atmconfig** - a FORE program used to enable or disable SPANS signalling.

**atmstat** - a FORE program that shows statistics gathered about a given adapter card by the device driver. These statistics include ATM layer and ATM adaptation layer cell and error counts. This can also be used to query other hosts via SNMP.

**AUI (Attachment User Interface)** - IEEE 802.3 interface between a media attachment unit (MAU) and a network interface card (NIC). The term AUI can also refer to the rear panel port to which an AUI cable might attach.

**Auto-logout** - a feature that automatically logs out a user if there has been no user interface activity for a specified length of time.

**B8ZS (Bipolar 8 Zero Substitution)** - a line coding technique used to accommodate the ones density requirements of T1 facilities.

**Backbone** - the main connectivity device of a distributed system. All systems that have connectivity to the backbone connect to each other. This does not stop systems from setting up private arrangements with each other to bypass the backbone for cost, performance, or security.

**Bandwidth** - usually identifies the capacity or amount of data that can be sent through a given circuit; may be user-specified in a PVC.

**baud** - unit of signalling speed. The speed in baud is the number of discrete conditions or signal events per second. If each signal event represents only one bit, the baud rate is the same as bps; if each signal event represents more than one bit (such as a dibit), the baud rate is smaller than bps.

**BECN (Backward Explicit Congestion Notification)** - bit set by a Frame Relay network in frames traveling in the opposite direction of frames encountering a congested path. Data terminal equipment (DTE) receiving frames with the BECN bit set can request that higher-level protocols take flow control action as appropriate. Compare with *FECN*.

**BES (Bursty Errored Seconds)** - a BES contains more than 1 and fewer than 320 path coding violation error events, and no severely errored frame or AIS defects. Controlled slips are not included in determining BESs.

**BGP (Border Gateway Protocol)** - used by gateways in an internet connecting autonomous networks. It is derived from experiences learned using the EGP.

**BIP (Bit Interleaved Parity)** - an error-detection technique in which character bit patterns are forced into parity, so that the total number of one bits is always odd or always even. This is accomplished by the addition of a one or zero bit to each byte, as the byte is transmitted; at the other end of the transmission, the receiving device verifies the parity (odd or even) and the accuracy of the transmission.

**B-ISDN (Broadband Integrated Services Digital Network)** - a common digital network suitable for voice, video, and high-speed data services running at rates beginning at 155 Mbps.

**BNC (Bayonet-Neill-Concelman)** - a bayonet-locking connector for miniature coax.

**BPDU (Bridged Protocol Data Unit)** - Spanning-tree Protocol hello packet that is sent out at configurable intervals to exchange information among bridges in the network.

**bps (bits per second)** - a measure of speed or data rate. Often combined with metric prefixes in kbps for thousands of bits per second (k fir kilo-) and in Mbps for millions of bits per second (M for mega-).

**BPV (Bipolar Violation)** - an error event on a line in which the normal pattern of alternating high (one) and low (zero) signals is disrupted. A bipolar violation is noted when two high signals occur without an intervening low signal, or vice versa.

**Bridge** - a device that expands a Local Area Network by forwarding frames between data link layers associated with two separate cables, usually carrying a common protocol. Bridges can usually be made to filter certain packets (to forward only certain traffic).

**Broadband** - a service or system requiring transmission channels capable of supporting rates greater than the Integrated Services Digital Network (ISDN) primary rate.

**Broadband Access** - an ISDN access capable of supporting one or more broadband services.

**Brouter (bridging/router)** - a device that routes some protocols and bridges others based on configuration information.

**Bursty Second** - a second during which there were at least the set number of BES threshold event errors but fewer than the set number of SES threshold event errors.

**BUS (Broadcast and Unknown Server)** - in an emulated LAN, the BUS is responsible for accepting broadcast, multicast, and unknown unicast packets from the LECs to the broadcast MAC address (FFFFFFFFFFFF) via dedicated point-to-point connections, and forwarding the packets to all of the members of the ELAN using a single point-to-multipoint connection.

**CAC (Connection Admission Control)** - the procedure used to decide if a request for an ATM connection can be accepted based on the attributes of both the requested connection and the existing connections.

**Call** - an association between two or more users or between a user and a network entity that is established by the use of network capabilities. This association may have zero or more connections.

**Carrier** - a company, such as any of the "baby Bell" companies, that provide network communications services, either within a local area or between local areas.

**CBR (Constant Bit Rate)** - a type of traffic that requires a continuous, specific amount of bandwidth over the ATM network (e.g., digital information such as video and digitized voice).

**CBR port** - a port on the *CellPath* 300 for transmitting and receiving CBR traffic.

**cchan** - a FORE program used to manage virtual channels on a FORE Systems ATM switch running asxd.

**CCITT (Consultative Committee for International Telephone and Telegraph)** - an international consultative committee that sets international communications recommendations, which are frequently adopted as standards; develops interface, modem, and data network recommendations. Membership includes PTTs, scientific and trade associations, and private companies. CCITT is part of the International Communications Union (a United nations treaty organization in Geneva).

**CDV (Cell Delay Variation)** - a quantification of cell clumping for a connection. The cell clumping CDV (yk) is defined as the difference between a cell's expected reference arrival time (ck) and its actual arrival time (ak). The expected reference arrival time (ck) of cell k of a specific connection is $\max [c_{\{k-1\}} + T, a_k]$. T is the reciprocal of the negotiated peak cell rate.

**CE (Connection Endpoint)** - a terminator at one end of a layer connection within a SAP.

**CEI (Connection Endpoint Identifier)** - an identifier of a CE that can be used to identify the connection at a SAP.

**Cell** - an ATM Layer protocol data unit (PDU). The basic unit of information transported in ATM technology, each 53-byte cell contains a 5-byte header and a 48-byte payload.

**Cell Delineation** - the protocol for recognizing the beginning and end of ATM cells within the raw serial bit stream.

**Cell Header** - ATM Layer protocol control information.

**Cell Port** - a port on the *CellPath* 300 that transmits and receives traffic in cell format.

**Cell Rate Adaptation** - a function performed by a protocol module in which empty cells (known as unassigned cells) are added to the output stream. This is because there always must be a fixed number of cells in the output direction; when there are not enough cells to transmit, unassigned cells are added to the output data stream.

**Cell Transfer Delay** - the transit delay of an ATM cell successfully passed between two designated boundaries.

**CES (Circuit emulation Services)** - The *CellPath* 90 supports Circuit Emulation Services (CES) for applications requiring a fixed delay, lossless end-to-end connection through the network. In essence, CES provides a virtual private line service to the connecting application.

**Channelization** - capability of transmitting independent signals together over a cable while still maintaining their separate identity for later separation.

**CLP (Cell Loss Priority)** - the last bit of byte four in an ATM cell header; indicates the eligibility of the cell for discard by the network under congested conditions. If the bit is set to 1, the cell may be discarded by the network depending on traffic conditions.

**Cold Start Trap** - a *CellPath* 300 SNMP trap which is sent when the unit has been power-cycled (*see* trap).

**Comm Port** - the front panel DCE port that allows access to the *CellPath* 300 user interface via a connected terminal.

**Concentrator** - a communications device that offers the ability to concentrate many lower-speed channels into and out of one or more high-speed channels.

**Congestion Management** - a *CellPath* 300 feature that helps ensure reasonable service for VBR connections in an ATM network. For each connection, the *CellPath* 300 maintains a priority, sustained cell rate (SCR), and peak cell rate (PCR). During times of congestion, the *CellPath* 300 reduces the bandwidth to the SCR, based on the priority of the connection.

**Connection** - the concatenation of ATM Layer links in order to provide an end-to-end information transfer capability to access points.

**Connectionless Service** - a type of service in which no pre-determined path or link has been established for transfer of information, supported by AAL 4.

**Connection-Oriented Service** - a type of service in which information always traverses the same pre-established path or link between two points, supported by AAL 3.

**Controlled Slip** - a situation in which one frame's worth of data is either lost or replicated. A controlled slip typically occurs when the sending device and receiving device are not using the same clock.

**Corresponding Entities** - peer entities with a lower layer connection among them.

**cpath** - a FORE program used to manage virtual paths on a FORE Systems ATM switch running asxd.

**CPE (Customer Premise Equipment)** - equipment that is on the customer side of the point of demarcation, as opposed to equipment that is on a carrier side. *See also* point of demarcation.

**cport** - a FORE program used to monitor and change the state of ports on a FORE Systems ATM switch running asxd.

**CRC (Cyclic Redundancy Check)** - an error detection scheme in which a number is derived from the data that will be transmitted. By recalculating the CRC at the remote end and comparing it to the value originally transmitted, the receiving node can detect errors.

**Cross Connection** - a mapping between two channels or paths at a network device such as the *CellPath* 300.

**CD (Controlled Slip)** - a situation in which one frame's worth of data is either lost or replicated. A controlled slip typically occurs when the sending device and receiving device are not using the same clock.

**CS (Convergence Sublayer)** - a portion of the AAL. Data is passed first to the CS where it is divided into rational, fixed-length packets or PDUs (Protocol Data Units). For example, AAL 4 processes user data into blocks that are a maximum of 64 kbytes long.

**CTS (Clear To Send)** - and RS-232 modem interface control signal (sent from the modem to the DTE on pin 5) which indicates that the attached DTE may begin transmitting; issuance in response to the DTE's RTS.

**D4 framing** - See SF)

**DARPA (Defense Advanced Research Projects Agency)** - the US government agency that funded the ARPANET.

**Datagram** - a packet of information used in a connectionless network service that is routed to its destination using an address included in the datagram's header.

**DCE (Data Communications Equipment)** - a definition in the RS232C standard that describes the functions of the signals and the physical characteristics of an interface for a communication device such as a modem.

**DCS (Digital Cross-connect System)** - an electronic patch panel used to route digital signals in a central office.

**Demultiplexing** - a function performed by a layer entity that identifies and separates SDUs from a single connection to more than one connection (*see* multiplexing).

**DFA (DXI Frame Address)** - a connection identifier associated with ATM DXI packets that serves the same functions as, and translates directly to, the VPI/VCI on an ATM cell.

**DIP Switch (Dual In-line Package)** - a device that has two parallel rows of contacts that let the user switch electrical current through a pair of those contacts to on or off. They are used to reconfigure components and peripherals.

**DLCI (Data Link Connection Identifier)** - a connection identifier associated with frame relay packets that serves the same functions as, and translates directly to, the VPI/VCI on an ATM cell.

**Domain Name Server** - a computer that converts names to their corresponding Internet numbers. It allows users to telnet or FTP to the name instead of the number.

**DNS (Domain Name System)** - the distributed name and address mechanism used in the Internet.

**DSn (Digital Standard n (0, 1, 1C, 2, and 3))** - a method defining the rate and format of digital hierarchy, with asynchronous data rates defined as follows:

| | | |
|---|---|---|
| DS0 | 64kbps | 1 voice channel |
| DS1 | 1.544Mbps | 24 DS0s |
| DS1C | 3.152 Mbps | 2 DS1s |
| DS2 | 6.312 Mbps | 4 DS1s |
| DS3 | 44.736 Mbps | 28 DS1s |

Synchronous data rates (SONET) are defined as:

| | | |
|---|---|---|
| STS-1/OC-1 | 51.84 Mbps | 28 DS1s or 1 DS3 |
| STS-3/OC-3 | 155.52 Mbps | 3 STS-1s byte interleaved |
| STS-3c/OC-3c | 155.52 Mbps | Concatenated, indivisible payload |
| STS-12/OC-12 | 622.08 Mbps | 12 STS-1s, 4 STS-3cs, or any mixture |
| STS-12c/OC-12c | 622.08 Mbps | Concatenated, indivisible payload |
| STS-48/OC-48 | 2488.32 Mbps | 48 STS-1s, 16 STS-3cs, or any mixture |

**DSR (Data Set Ready)** - an RS-232 modem interface control signal (sent from the modem to the DTE on pin 6) which indicates that the modem is connected to the telephone circuit. Usually a prerequisite to the DTE issuing RTS.

**DTE (Data Terminal Equipment)** - generally user devices, such as terminals and computers, that connect to data circuit-terminating equipment. They either generate or receive the data carried by the network.

**DTR (Data Terminal Ready)** - an RS232 modem interface control signal (sent from the DTE to the modem on pin 20) which indicates that the DTE is ready for data transmission and which requests that the modem be connected to the telephone circuit.

**DXI** - a generic phrase used in the full names of several protocols, all commonly used to allow a pair of DCE and DTE devices to share the implementation of a particular WAN protocol. The protocols all define the packet formats used to transport data packets between DCE and DTE devices.

**E1** - Wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 2.048 Mbps. E1 lines can be leased for private use from common carriers.

**E3** - Wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 34.368 Mbps. E3 lines can be leased for private use from common carriers.

**EEPROM (Electrically Erasable Programmable Read Only Memory)** - an EPROM that can be cleared with electrical signals rather than the traditional ultraviolet light.

**EFCI (Explicit Forward Congestion Indication)** - the second bit of the payload type field in the header of an ATM cell, the EFCI bit indicates network congestion to receiving hosts. On a congested switch, the EFCI bit is set to "1" by the transmitting network module when a certain number of cells have accumulated in the network module's shared memory buffer. When a cell is received that has its EFCI bit set to "1," the receiving host notifies the sending host, which should then reduce its transmission rate.

**EGP (Exterior Gateway) Protocol** - used by gateways in an internet, connecting autonomous networks.

**EIA (Electronics Industries Association)** - a USA trade organization that issues its own standards and contributes to ANSI; developed RS-232. Membership includes USA manufacturers.

**EISA (Extended Industry Standard Architecture)** - a bus architecture for desktop computers that provides a 32-bit data passage while maintaining compatibility with the ISA or AT architecture.

**elarp** - a FORE program that shows and manipulates MAC and ATM address mappings for LAN Emulation Clients (LECs).

**elconfig** - a FORE program that shows and modifies LEC configuration. Allows the user to set the NSAP address of the LAN Emulation Configuration Server (LECS), display the list of Emulated LANs (ELANs) configured in the LECS for this host, display the list of ELANs locally configured along with the membership state of each, and locally administer ELAN membership.

**EM** - the *CellPath* 300 extension module; paired with the system controller and supporting an optional PCMCIA card.

**Embedded SNMP Agent** - an SNMP agent can come in two forms: embedded or proxy. An embedded SNMP agent is integrated into the physical hardware and software of the unit. The *CellPath* 300 has an internal, integrated SNMP agent.

**EMI (Electromagnetic Interference)** - signals generated and radiated by an electronic device that cause interference with radio communications, among other effects.

**End-to-End Connection** - when used in reference to an ATM network, a connection that travels through an ATM network, passing through various ATM devices and with endpoints at the termination of the ATM network.

**EPROM** - Erasable Programmable Read Only Memory (*see* PROM).

**EQL (Equalization)** - the process of compensating for line distortions.

**ES (End System)** - a system in which an ATM connection is terminated or initiated. An originating end system initiates the ATM connection, and a terminating end system terminates the ATM connection. OAM cells may be generated and received.

**ES (Errored Seconds)** - a second during which at least one code violation occurred.

**ESF (Extended Superframe)** - T1 framing standard that provides frame synchronization, cyclic redundancy, and data link bits.

**Ethernet** - a 10-Mbps, coaxial standard for LANs in which all nodes connect to the cable where they contend for access.

**Fairness** - as related to Generic Flow Control (GFC), fairness is defined as meeting all of the agreed quality of service (QoS) requirements by controlling the order of service for all active connections.

**Far-End** - in a relationship between two devices in a circuit, the far-end device is the one that is remote.

**FCC** - a board of commissioners appointed by the President under the Communications Act of 1934, with the authority to regulate all interstate telecommunications originating in the United States, including transmission over phone lines.

**FDDI (Fiber Distributed Data Interface)** - high-speed data network that uses fiber-optic as the physical medium. Operates in similar manner to Ethernet or Token Ring, only faster.

**FDM (Frequency Division Multiplexing)** - a method of dividing an available frequency range into parts with each having enough bandwidth to carry one channel.

**FEBE (Far End Block Error)** - an error detected by extracting the 4-bit FEBE field from the path status byte (G1). The legal range for the 4-bit field is between 0000 and 1000, representing zero to eight errors. Any other value is interpreted as zero errors.

**FECN (Forward Explicit Congestion Notification)** - bit set by a Frame Relay network to inform data terminal equipment (DTE) receiving the frame that congestion was experienced in the path from source to destination. DTE receiving frames with the FECN bit set can request that higher-level protocols take flow control action as appropriate. Compare with *BECN*.

**FERF (Far End Receive Failure)** - a line error asserted when a 110 binary pattern is detected in bits 6, 7, 8 of the K2 byte for five consecutive frames. A line FERF is removed when any pattern other than 110 is detected in these bits for five consecutive frames.

**FIFO (First-In, First-Out)** - a method of coordinating the sequential flow of data through a buffer.

**Flag** - a specific bit pattern used to identify the beginning or end of a frame.

**Frame** - a variable length group of data bits with a specific format containing flags at the beginning and end to provide demarcation.

**Frame Relay** - a fast packet switching protocol based on the LAPD protocol of ISDN that performs routing and transfer with less overhead processing than X.25.

**Frame Synchronization Error** - an error in which one or more time slot framing bits are in error.

**Framing** - a protocol that separates incoming bits into identifiable groups so that the receiving multiplexer recognizes the grouping.

**FT-PNNI (ForeThought PNNI)** - a FORE Systems routing and signalling protocol that uses private ATM (NSAP) addresses; a precursor to ATM Forum PNNI (*see* PNNI).

**FTP (File Transfer Protocol)** - a TCP/IP protocol that lets a user on one computer access, and transfer data to and from, another computer over a network. ftp is usually the name of the program the user invokes to accomplish this task.

**GCRA (Generic Cell Rate Algorithm)** - an algorithm which is employed in traffic policing and is part of the user/network service contract. The GCRA is a scheduling algorithm which ensures that cells are marked as *conforming* when they arrive when expected or later than expected and *non-conforming* when they arrive sooner than expected.

**GFC (Generic Flow Control)** - the first four bits of the first byte in an ATM cell header. Used to control the flow of traffic across the User-to-Network Interface (UNI), and thus into the network. Exact mechanisms for flow control are still under investigation and no explicit definition for this field exists at this time. (This field is used only at the UNI; for NNI-NNI use (between network nodes), these four bits provide additional network address capacity, and are appended to the VPI field.)

**GIO** - a proprietary bus architecture used in certain Silicon Graphics, Inc. workstations.

**Header** - protocol control information located at the beginning of a protocol data unit.

**HDB3 (High Density Bipolar)** - line-code type standard for T1 where each block of three zeros is replaced by 00V or B0V, where B represents an inserted pulse conforming to the AMI rule (ITU-T G.701, item 9004) and V represents an AMI violation (ITU-T G.701, item 9007). The choice of 00V or B0V is made so that the number of B pulses between consecutive V pulses is odd (successive V pulses are of alternate polarity so that no d.c. component is introduced). Compare with *AMI*.

**HDLC (High-Level Data Link Control)** - Bit-oriented synchronous data link layer protocol developed by the ISO. Derived from SDLC, HDLC specifies a data encapsulation method on synchronous serial links using frame characters and checksums. See also *SDLC*.

**HEC (Header Error Control)** - a CRC code located in the last byte of an ATM cell header that is used for checking cell integrity only.

**HIPPI (High Performance Parallel Interface)** - ANSI standard that extends the computer bus over fairly short distances at speeds of 800 and 1600 Mbps.

**HPUX** - the Hewlett-Packard version of UNIX.

**HSSI (High-Speed Serial Interface)** - a serial communications connection that operates at speeds of up to 1.544 Mbps.

**Hub** - a device that connects several other devices, usually in a star topology.

I/O Module - FORE's interface cards for the LAX-20 LAN Access Switch, designed to connect Ethernet, Token Ring, and FDDI LANs to *ForeRunner* ATM networks.

**ICMP (Internet Control Message Protocol)** - the protocol that handles errors and control messages at the IP layer. ICMP is actually a part of the IP protocol layer. It can generate error messages, test packets, and informational messages related to IP.

**IEEE (Institute of Electrical and Electronics Engineers)** - the world's largest technical professional society. Based in the U.S., the IEEE sponsors technical conferences, symposia & local meetings worldwide, publishes nearly 25% of the world's technical papers in electrical, electronics & computer engineering, provides educational programs for members, and promotes standardization.

**IETF (Internet Engineering Task Force)** - a large, open, international community of network designers, operators, vendors and researchers whose purpose is to coordinate the operation, management and evolution of the Internet to resolve short- and mid-range protocol and architectural issues.

**ILMI (Interim Local Management Interface)** - the standard that specifies the use of the Simple Network Management Protocol (SNMP) and an ATM management information base (MIB) to provide network status and configuration information.

**Interface Data** - the unit of information transferred to/from the upper layer in a single interaction across a SAP. Each Interface Data Unit (IDU) controls interface information and may also contain the whole or part of the SDU.

**internet** - while an internet is a network, the term "internet" is usually used to refer to a collection of networks interconnected with routers.

**Internet** - (note the capital "I") the largest internet in the world including large national backbone nets and many regional and local networks worldwide. The Internet uses the TCP/IP suite. Networks with only e-mail connectivity are not considered on the Internet.

**Internet Addresses** - the numbers used to identify hosts on an internet network. Internet host numbers are divided into two parts; the first is the network number and the second, or local, part is a host number on that particular network. There are also three classes of networks in the Internet, based on the number of hosts on a given network. Large networks are classified as Class A, having addresses in the range 1-126 and having a maximum of 16,387,064 hosts. Medium networks are classified as Class B, with addresses in the range 128-191 and with a maximum of 64,516 hosts. Small networks are classified as Class C, having addresses in the range 192-254 with a maximum of 254 hosts. Addresses are given as dotted decimal numbers in the following format:

nnn.nnn.nnn.nnn

In a Class A network, the first of the numbers is the network number, the last three numbers are the local host address.

In a Class B network, the first two numbers are the network, the last two are the local host address.

In a Class C network, the first three numbers are the network address, the last number is the local host address.

The following table summarizes the classes and sizes:

| Class | First # | Max# Hosts |
|---|---|---|
| A | 1-126 | 16,387,064 |
| B | 129-191 | 64,516 |
| C | 192-223 | 254 |

Network mask values are used to identify the network portion and the host portion of the address. For:

Class A - the default mask is 255.0.0.0

Class B - the default mask is 255.255.0.0

Class C - the default mask is 255.255.255.0

Subnet masking is used when a portion of the host ID is used to identify a subnetwork. For example, if a portion of a Class B network address is used for a subnetwork, the mask could be set as 255.255.255.0. This would allow the third byte to be used as a subnetwork address. All hosts on the network would still use the IP address to get on the Internet.

**IP (Internet Protocol)** - a connectionless, best-effort packet switching protocol that offers a common layer over dissimilar networks.

**IP Address** - a unique 32-bit integer used to identify a device in an IP network. You will most commonly see IP addresses written in “dot” notation; for instance, 192.228.32.14 (*see* IP net-mask).

**IP Netmask** - a pattern of 32 bits that is combined with an IP address to determine which bits of an IP address denote the network number and which denote the host number. Netmasks are useful for sub-dividing IP networks. IP netmasks are written in "dot" notation; for instance, 255.255.255.0 (*see* IP address).

**IPX Protocol (Internetwork Packet Exchange)** - a NetWare protocol similar to the Xerox Network Systems (XNS) protocol that provides datagram delivery of messages.

**IS (Intermediate system)** - a system that provides forwarding functions or relaying functions or both for a specific ATM connection. OAM cells may be generated and received.

**ISA Bus** - a bus standard developed by IBM for expansion cards in the first IBM PC. The original bus supported a data path only 8 bits wide. IBM subsequently developed a 16-bit version for its AT class computers. The 16-bit AT ISA bus supports both 8- and 16-bit cards. The 8-bit bus is commonly called the PC / XT bus, and the 16-bit bus is called the AT bus.

**ISDN (Integrated Services Digital Network)** - an emerging technology that is beginning to be offered by the telephone carriers of the world. ISDN combines voice and digital network services into a single medium or wire.

**ISO (International Standards Organization)** - a voluntary, non treaty organization founded in 1946 that is responsible for creating international standards in many areas, including computers and communications.

**Isochronous** - signals carrying embedded timing information or signals that are dependent on uniform timing; usually associated with voice and / or video transmission.

**ITU (International Telecommunications Union)** - the telecommunications agency of the United Nations, established to provide standardized communications procedures and practices, including frequency allocation and radio regulations, on a worldwide basis.

**J2** - Wide-area digital transmission scheme used predominantly in Japan that carries data at a rate of 6.312 Mbps.

**Jitter** - analog communication line distortion caused by variations of a signal from its reference timing position.

**Jumper** - a patch cable or wire used to establish a circuit, often temporarily, for testing or diagnostics; also, the devices, shorting blocks, used to connect adjacent exposed pins on a printed circuit board that control the functionality of the card.

**LAN (Local Area Network)** - a data network intended to serve an area of only a few square kilometers or less. Because the network is known to cover only a small area, optimizations can be made in the network signal protocols that permit higher data rates.

**lane** - a program that provides control over the execution of the LAN Emulation Server (LES), Broadcast / Unknown Server (BUS), and LAN Emulation Configuration Server (LECS) on the local host.

**LAN Access Concentrator** - a LAN access device that allows a shared transmission medium to accommodate more data sources than there are channels currently available within the transmission medium.

**LAPB (Link Access Procedure, Balanced)** - Data link protocol in the X.25 protocol stack. LAPB is a bit-oriented protocol derived from HDLC. See also HDLC and X.25.

**LAX-20** - a FORE Systems LAN Access Switch, designed to connect Ethernet, Token Ring, and FDDI LANs to *ForeRunner* ATM networks. The LAX-20 is a multiport, multiprotocol internetworking switch that combines the advantages of a high-performance LAN switch and a full-featured ATM interface capable of carrying LAN traffic.

**Layer Entity** - an active layer within an element.

**Layer Function** - a part of the activity of the layer entities.

**Layer Service** - a capability of a layer and the layers beneath it that is provided to the upper layer entities at the boundary between that layer and the next higher layer.

**Layer User Data** - the information transferred between corresponding entities on behalf of the upper layer or layer management entities for which they are providing services.

**le** - a FORE program that implements both the LAN Emulation Server (LES) and the Broadcast / Unknown Server (BUS).

**LEC (LAN Emulation Client)** - the component in an end system that performs data forwarding, address resolution, and other control functions when communicating with other components within an ELAN.

**lecs** - a FORE program that implements the assignment of individual LECs to different emulated LANs.

**LECS (LAN Emulation Configuration Server)** - the LECS is responsible for the initial configuration of LECs. It provides information about available ELANs that a LEC may join, together with the addresses of the LES and BUS associated with each ELAN.

**leq** - a FORE program that provides information about an ELAN. This information is obtained from the LES, and includes MAC addresses registered on the ELAN together with their corresponding ATM addresses.

**LES (LAN Emulation Server)** - the LES implements the control coordination function for an ELAN. The LES provides the service of registering and resolving MAC addresses to ATM addresses.

**Link Down Trap** - a *CellPath* 300 SNMP trap that signifies that the Ethernet interface has transitioned from a normal state to an error state, or has been disconnected.

**Link Up Trap** - a *CellPath* 300 SNMP trap that signifies that the Ethernet interface has transitioned from an error condition to a normal state.

**LLC (Logical Link Control)** - a protocol developed by the IEEE 802 committee for data-link-layer transmission control; the upper sublayer of the IEEE Layer 2 (OSI) protocol that complements the MAC protocol; IEEE standard 802.2; includes end-system addressing and error checking.

**LOF (Loss Of Frame)** - a type of transmission error that may occur in wide-area carrier lines.

**Loopback** - a troubleshooting technique that returns a transmitted signal to its source so that the signal can be analyzed for errors. Typically, a loopback is set at various points in a line until the section of the line that is causing the problem is discovered.

**looptest** - a program that tests the interface for basic cell reception and transmission functionality. It is usually used for diagnostic purposes to determine if an interface is functioning properly.

**LOP (Loss Of Pointer)** - a type of transmission error that may occur in wide-area carrier lines.

**LOS (Loss Of Signal)** - a type of transmission error that may occur in wide-area carrier lines.

**MAC (Media Access Control)** - a media-specific access control protocol within IEEE 802 specifications; currently includes variations for Token Ring, token bus, and CSMA/CD; the lower sublayer of the IEEE's link layer (OSI), which complements the Logical Link Control (LLC).

**MAU (Media Attachment Unit)** - device used in Ethernet and IEEE 802.3 networks that provides the interface between the AUI port of a station and the common medium of the Ethernet. The MAU, which can be built into a station or can be a separate device, performs physical layer functions including conversion of the digital data from the Ethernet interface, collision detection, and injection of bits onto the network.

**Maximum Burst Tolerance** - the largest burst of data that a network device is guaranteed to handle without discarding cells or packets. Bursts of data larger than the maximum burst size may be subject to discard.

**MCR (Minimum Cell Rate)** - parameter defined by the ATM Forum for ATM traffic management. MCR is defined only for ABR transmissions, and specifies the minimum value for the ACR.

**Metasignalling** - an ATM Layer Management (LM) process that manages different types of signalling and possibly semipermanent virtual channels (VCs), including the assignment, removal, and checking of VCs.

**Metasignalling VCs** - the standardized VCs that convey metasignalling information across a User-to-Network Interface (UNI).

**MIB (Management Information Base)** - the set of parameters that an SNMP management station can query or set in the SNMP agent of a networked device (e.g., router).

**MIC (Media Interface Connector)** - the optical fiber connector that joins the fiber to the FDDI controller.

**MicroChannel** - a proprietary 16- or 32-bit bus developed by IBM for its PS/2 computers' internal expansion cards; also offered by others.

**MTU (Maximum Transmission Unit)** - the largest unit of data that can be sent over a type of physical medium.

**Multi-homed** - a device that has both an ATM and another network connection, typically Ethernet.

**Multiplexing** - a function within a layer that interleaves the information from multiple connections into one connection (*see* demultiplexing).

**Multipoint Access** - user access in which more than one terminal equipment (TE) is supported by a single network termination.

**Multipoint-to-Point Connection** - a Point-to-Multipoint Connection may have zero bandwidth from the Root Node to the Leaf Nodes, and non-zero return bandwidth from the Leaf Nodes to the Root Node. Such a connection is also known as a Multipoint-to-Point Connection.

**Multipoint-to-Multipoint Connection** - a collection of associated ATM VC or VP links, and their associated endpoint nodes, with the following properties:

1. All N nodes in the connection, called Endpoints, serve as a Root Node in a Point-to-Multipoint connection to all of the (N-1) remaining endpoints.

2. Each of the endpoints can send information directly to any other endpoint, but the receiving endpoint cannot distinguish which of the endpoints is sending information without additional (e.g., higher layer) information.

**Near-End** - in a relationship between two devices in a circuit, the near-end device is the one that is local.

**Network Module** - ATM port interface cards which may be individually added or removed from any *ForeRunner* ATM switch to provide a diverse choice of connection alternatives. Each network module provides between one and six full-duplex ATM physical connections to the *ForeRunner* switch.

**NMS (Network Management Station)** - the system responsible for managing a network or a portion of a network. The NMS talks to network management agents, which reside in the managed nodes.

**NNI (Network-to-Network Interface or Network Node Interface)** - the interface between two public network pieces of equipment.

**nonvolatile** - a term used to describe a data storage device (memory) that retains its contents when power is lost.

**NuBus -** a high-speed bus used in the Macintosh family of computers, structured so that users can put a card into any slot on the board without creating conflict over the priority between those cards

**OAM (Operation and Maintenance) Cell** - a cell that contains ATM LM information. It does not form part of the upper layer information transfer.

**octet** - a grouping of 8 bits; similar, but not identical, to a byte.

**OID (Object Identifier)** - the address of a MIB variable.

**OOF (Out-of-Frame)** - a signal condition and alarm in which some or all framing bits are lost.

**OpenView** - Hewlett-Packard's network management software.

**OSI (Open Systems Interconnection)** - the 7-layer suite of protocols designed by ISO committees to be the international standard computer network architecture.

**OSPF (Open Shortest Path First) Protocol** - a routing algorithm for IP that incorporates least-cost, equal-cost, and load balancing.

**Out-of-Band Management** - refers to switch configuration via the serial port or over Ethernet, not ATM.

**packet** - a group of bits - including information bits and overhead bits - transmitted as a complete package on a network. Usually smaller than a transmission block.

**Packet Port** - a port on the *CellPath* 300 that transmits and receives packet traffic.

**Packet Switching** - a communications paradigm in which packets (messages) are individually routed between hosts with no previously established communications path.

**Payload Scrambling** - a technique that eliminates certain bit patterns that may occur within an ATM cell payload that could be misinterpreted by certain sensitive transmission equipment as an alarm condition.

**PBX (Private Branch Exchange)** - a private phone system (switch) that connects to the public telephone network and offers in-house connectivity. To reach an outside line, the user must dial a digit like 8 or 9.

**PCI (Peripheral Component Interconnect)** - a local-bus standard created by Intel.

**PCM (Pulse Code Modulation)** - a modulation scheme that samples the information signals and transmits a series of coded pulses to represent the data.

**PCR (Peak Cell Rate)** - parameter defined by the ATM Forum for ATM traffic management. In CBR transmissions, PCR determines how often data samples are sent. In ABR transmissions, PCR determines the maximum value of the ACR.

**PDN (Public Data Network)** - a network designed primarily for data transmission and intended for sharing by many users from many organizations.

**PDU (Protocol Data Unit)** - a unit of data specified in a layer protocol and consisting of protocol control information and layer user data.

**Peak Cell Rate** - at the PHY Layer SAP of a point-to-point VCC, the Peak Cell Rate Rpis the inverse of the minimum inter-arrival time T0 of the request to send an ATM-SDU.

**Peer Entities** - entities within the same layer.

**PHY (Physical Layer)** - the actual cards, wires, and/or fiber-optic cabling used to connect computers, routers, and switches.

**Physical Layer (PHY) Connection** - an association established by the PHY between two or more ATM-entities. A PHY connection consists of the concatenation of PHY links in order to provide an end-to-end transfer capability to PHY SAPs.

**PLCP (Physical Layer Convergence Protocol)** - a framing protocol that runs on top of the T1 or E1 framing protocol.

**PLM (Physical Layer Module)** - interface card in the *CellPath* 300 that provides the logic to support the physical layer of the network link. A PLM has the actual physical port mounted on it. Various PLMs support various physical layers, such as OC-3c/STM1 or DS3.

**PLP (Packet Level Protocol)** - Network layer protocol in the X.25 protocol stack. Sometimes called X.25 Level 3 or X.25 Protocol. See also X.25.

**PM (Protocol Module)** - interface card in the *CellPath* 300 that provides the logic supporting the protocol layer of the network link. Various PMs support various protocols, such as ATM cell, Frame Relay, or CBR traffic.

**PMD (Physical Medium Dependent)** - a sublayer concerned with the bit transfer between two network nodes. It deals with wave shapes, timing recovery, line coding, and electro-optic conversions for fiber based links.

**PNNI (Private Network Node Interface or Private Network-to-Network Interface)** - a protocol that defines the interaction of private ATM switches or groups of private ATM switches

**ping (Packet Internet Groper)** - a program used to test reachability of destinations by sending them an ICMP echo request and waiting for a reply.

**Point-to-Multipoint Connection** - a collection of associated ATM VC or VP links, with associated endpoint nodes, with the following properties:

1. One ATM link, called the Root Link, serves as the root in a simple tree topology. When the Root node sends information, all of the remaining nodes on the connection, called Leaf nodes, receive copies of the information.

2. Each of the Leaf Nodes on the connection can send information directly to the Root Node. The Root Node cannot distinguish which Leaf is sending information without additional (higher layer) information. (See the following note for Phase 1.)

3. The Leaf Nodes cannot communicate directly to each other with this connection type.

Note: Phase 1 signalling does not support traffic sent from a Leaf to the Root.

**Point-to-Point Connection** - a connection with only two endpoints.

**Point of Demarcation** - the dividing line between a carrier and the customer premise that is governed by strict standards that define the characteristics of the equipment on each side of the demarcation. Equipment on one side of the point of demarcation is the responsibility of the customer. Equipment on the other side of the point of demarcation is the responsibility of the carrier.

**Policing** - the function that ensures that a network device does not accept traffic that exceeds the configured bandwidth of a connection.

**Primitive** - an abstract, implementation-independent interaction between a layer service user and a layer service provider.

**Priority** - the parameter of ATM connections that determines the order in which they are reduced from the peak cell rate to the sustained cell rate in times of congestion. Connections with lower priority (4 is low, 1 is high) are reduced first.

**PROM (Programmable Read-Only Memory)** - a chip-based information storage area that can be recorded by an operator but erased only through a physical process.

**Protocol** - a set of rules and formats (semantic and syntactic) that determines the communication behavior of layer entities in the performance of the layer functions.

**Protocol Control Information** - the information exchanged between corresponding entities using a lower layer connection to coordinate their joint operation.

**Proxy** - the process in which one system acts for another system to answer protocol requests.

**Proxy Agent** - an agent that queries on behalf of the manager, used to monitor objects that are not directly manageable.

**PSN (Packet Switched Network)** - a network designed to carry data in the form of packets. The packet and its format is internal to that network.

**PT (Payload Type)** - bits 2...4 in the fourth byte of an ATM cell header. The PT indicates the type of information carried by the cell. At this time, values 0...3 are used to identify various types of user data, values 4 and 5 indicate management information, and values 6 and 7 are reserved for future use.

**PVC (Permanent Virtual Circuit (or Channel))** - a circuit or channel through an ATM network provisioned by a carrier between two endpoints; used for dedicated long-term information transport between locations.

**Q.2931** - Derived from Q.93B, the narrowband ISDN signalling protocol, an ITU standard describing the signalling protocol to be used by switched virtual circuits on ATM LANs.

**Real-Time Clock** - a clock that maintains the time of day, in contrast to a clock that is used to time the electrical pulses on a circuit.

**Relaying** - a function of a layer by means of which a layer entity receives data from a corresponding entity and transmits it to another corresponding entity.

**RFCs (Requests For Comment)** - IETF documents suggesting protocols and policies of the Internet, inviting comments as to the quality and validity of those policies. These comments are collected and analyzed by the IETF in order to finalize Internet standards.

**RFI (Radio Frequency Interference)** - the unintentional transmission of radio signals. Computer equipment and wiring can both generate and receive RFI.

**RIP (Routing Information Protocol)** - a distance vector-based protocol that provides a measure of distance, or hops, from a transmitting workstation to a receiving workstation.

**RISC (Reduced Instruction Set Computer)** - a generic name for CPUs that use a simpler instruction set than more traditional designs.

**Router** - a device that forwards traffic between networks or subnetworks based on network layer information.

**RTS (Request To Send)** - an RS-232 modem interface signal (sent from the DTE to the modem on pin 4) which indicates that the DTE has data to transmit.

**SBus** - hardware interface for add-in boards in later-version Sun 3 workstations.

**SAP (Service Access Point) -** the point at which an entity of a layer provides services to its LM entity or to an entity of the next higher layer.

**SAR (Segmentation And Reassembly)** - the SAR accepts PDUs from the CS and divides them into very small segments (44 bytes long). If the CS-PDU is less than 44 bytes, it is padded to 44 with zeroes. A two-byte header and trailer are added to this basic segment. The header identifies the message type (beginning, end, continuation, or single) and contains sequence numbering and message identification. The trailer gives the SAR-PDU payload length, exclusive of pad, and contains a CRC check to ensure the SAR-PDU integrity. The result is a 48-byte PDU that fits into the payload field of an ATM cell.

**SC** - *CellPath* 300 System Controller; paired with the Extension Module (EM).

**SCR (sustainable cell rate) -** parameter defined by the ATM Forum for ATM traffic management. For VBR connections, SCR determines the long-term average cell rate that can be transmitted.

**SCSI (Small Computer Systems Interface)** - a standard for a controller bus that connects disk drives and other devices to their controllers on a computer bus. It is typically used in small systems.

**SDLC (Synchronous Data Link Control)** - IBM's data link protocol used in SNA networks.

**SDU (Service Data Unit)** - a unit of interface information whose identity is preserved from one end of a layer connection to the other.

**SEAL (Simple and Efficient Adaptation Layer)** - also called AAL 5, this ATM adaptation layer assumes that higher layer processes will provide error recovery, thereby simplifying the SAR portion of the adaptation layer. Using this AAL type packs all 48 bytes of an ATM cell information field with data. It also assumes that only one message is crossing the UNI at a time. That is, multiple end-users at one location cannot interleave messages on the same VC, but must queue them for sequential transmission.

**Segment** - a single ATM link or group of interconnected ATM links of an ATM connection.

**Semipermanent Connection** - a connection established via a service order or via network management.

**SES (Severely Errored Seconds)** - a second during which more event errors have occurred than the SES threshold.

**SF (Superframe)** - Common framing type used on T1 circuits. SF consists of 12 frames of 192 bits each, with the 193rd bit providing error checking and other functions. SF has been superseded by ESF, but is still widely used. Also called *D4 framing*. See also ESF.

**SGMP (Simple Gateway Management Protocol)** - the predecessor to SNMP.

**Shaping Descriptor** - *n* ordered pairs of GCRA parameters (I,L) used to define the negotiated traffic shape of an APP connection. The traffic shape refers to the load-balancing of a network. In this context, load-balancing means configuring the data flows to maximize the efficiency of the network.

**SIR (Sustained Information Rate)** - the long-term average data transmission rate across the User-to-Network Interface.

**SMDS (Switched Multimegabit Data Service)** - a high-speed, datagram-based, public data network service expected to be widely used by telephone companies in their data networks.

**SMTP (Simple Mail Transfer Protocol)** - the Internet electronic mail protocol used to transfer electronic mail between hosts.

**SNAP** - SubNetwork Access Protocol

**SNMP (Simple Network Management Protocol)** - the Internet standard protocol for managing nodes on an IP network.

**snmpd** - an SMNP agent for a given adapter card.

**SONET (Synchronous Optical Network)** - a new and growing body of standards that defines all aspects of transporting and managing digital traffic over optical facilities in the public network.

**Source Traffic Descriptor** - a set of traffic parameters belonging to the ATM Traffic Descriptor used during the connection set-up to capture the intrinsic traffic characteristics of the connection requested by the source.

**Spanning Tree Protocol** - provides loop-free topology in a network environment where there are redundant paths.

**SPANS (Simple Protocol for ATM Network Signalling)** - FORE Systems' proprietary signalling protocol used for establishing SVCs between FORE Systems equipment.

**SPARC (Scalable Processor Architecture Reduced instruction set Computer)** - a powerful workstation similar to a reduced-instruction-set-computing (RISC) workstation.

**SPE (Synchronous Payload Envelope)** - the payload field plus a little overhead of a basic SONET signal.

**SPVC (Smart PVC)** - a generic term for any communications medium which is permanently provisioned at the end points, but switched in the middle. In ATM, there are two kinds of SPVCs: smart permanent virtual path connections (SPVPCs) and smart permanent virtual channel connections (SPVCCs).

**Static Route** - a route that is entered manually into the routing table.

**Statistical Multiplexing** - a technique for allowing multiple channels and paths to share the same link, typified by the ability to give the bandwidth of a temporarily idle channel to another channel.

**STM (Synchronous Transfer Mode)** - a transport and switching method that depends on information occurring in regular and fixed patterns with respect to a reference such as a frame pattern.

**STP (Shielded Twisted Pair)** - two or more insulated wires that are twisted together and then wrapped in a cable with metallic braid or foil to prevent interference and offer noise-free transmissions.

**STS (Synchronous Transport Signal)** - a SONET electrical signal rate.

**Sublayer** - a logical subdivision of a layer.

**Super User** - a login ID that allows unlimited access to the full range of a device's functionality, including especially the ability to reconfigure the device and set passwords.

**SVC (Switched Virtual Circuit (or Channel))** - a channel established on demand by network signalling, used for information transport between two locations and lasting only for the duration of the transfer; the datacom equivalent of a dialed telephone call.

**Switched Connection** - a connection established via signalling.

**Symmetric Connection** - a connection with the same bandwidth value specified for both directions.

**Synchronous** - signals that are sourced from the same timing reference and hence are identical in frequency.

**Systems Network Architecture (SNA)** - a proprietary networking architecture used by IBM and IBM-compatible mainframe computers.

**T1** - a specification for a transmission line. The specification details the input and output characteristics and the bandwidth. T1 lines run at 1.544 Mbps and provide for 24 data channels. In common usage, the term "T1" is used interchangeably with "DS1."

**T3** - a specification for a transmission line, the equivalent of 28 T1 lines. T3 lines run at 44.736 Mbps. In common usage, the term "T3" is used interchangeably with "DS3."

**Tachometer** - in *ForeView*, the tachometer shows the level of activity on a given port. The number in the tachometer shows the value of a chosen parameter in percentage, with a colored bar providing a semi-logarithmic representation of that percentage.

**TAXI (Transparent Asynchronous Transmitter/Receiver Interface)** - Encoding scheme used for FDDI LANs as well as for ATM; supports speeds of up to 100 Mbps over multimode fiber.

**TC (Transmission Convergence)** - generates and receives transmission frames and is responsible for all overhead associated with the transmission frame. The TC sublayer packages cells into the transmission frame.

**TCP (Transmission Control Protocol)** - a specification for software that bundles and unbundles sent and received data into packets, manages the transmission of packets on a network, and checks for errors.

**TCP/IP (Transmission Control Protocol/Internet Protocol)** - a set of communications protocols that has evolved since the late 1970s, when it was first developed by the Department of Defense. Because programs supporting these protocols are available on so many different computer systems, they have become an excellent way to connect different types of computers over networks.

**TDM (Time Division Multiplexing)** - a method of traditional digital multiplexing in which a signal occupies a fixed, repetitive time slot within a higher-rate signal.

**Telnet** - a TCP/IP protocol that defines a client/server mechanism for emulating directly-connected terminal connections.

**Token Ring** - a network access method in which the stations circulate a token. Stations with data to send must have the token to transmit their data.

**topology** - a program that displays the topology of a FORE Systems ATM network. An updated topology can be periodically re-displayed by use of the interval command option.

**Traffic** - the calls being sent and received over a communications network. Also, the packets that are sent on a data network.

**Trailer** - the protocol control information located at the end of a PDU.

**Transit Delay** - the time difference between the instant at which the first bit of a PDU crosses one designated boundary, and the instant at which the last bit of the same PDU crosses a second designated boundary.

**trap** - a program interrupt mechanism that automatically updates the state of the network to remote network management hosts. The SNMP agent on the switch supports these SNMP traps.

**UAS (Unavailable Seconds)** - a measurement of signal quality. Unavailable seconds start accruing when ten consecutive severely errored seconds occur.

**UBR (Unspecified Bit Rate)** - a type of traffic that is not considered time-critical (e.g., ARP messages, pure data), allocated whatever bandwidth is available at any given time. UBR traffic is given a "best effort" priority in an ATM network with no guarantee of successful transmission.

**UDP (User Datagram Protocol)** - the TCP/IP transaction protocol used for applications such as remote network management and name-service access; this lets users assign a name, such as "RVAX*2,S," to a physical or numbered address.

**Unassigned Cells** - a generated cell identified by a standardized virtual path identifier (VPI) and virtual channel identifier (VCI) value, which does not carry information from an application using the ATM Layer service.

**UNI (User-to-Network Interface)** - the physical and electrical demarcation point between the user and the public network service provider.

**UNI 3.0** - the User-to-Network Interface standard set forth by the ATM Forum that defines how private customer premise equipment interacts with private ATM switches.

**UPC (Usage Parameter Control)** - the mechanism that ensures that traffic on a given connection does not exceed the contracted bandwidth of the connection. UPC is responsible for policing or enforcement. UPC is sometimes confused with congestion management, to which it is functionally related on the *CellPath* 300 (*see* congestion management).

**UTP (Unshielded Twisted Pair)** - a cable that consists of two or more insulated conductors in which each pair of conductors are twisted around each other. There is no external protection and noise resistance comes solely from the twists.

**V.35** - ITU-T standard describing a synchronous, physical layer protocol used for communications between a network access device and a packet network. V.35 is most commonly used in the United States and Europe, and is recommended for speeds up to 48 Kbps.

**VBR (Variable Bit Rate)** - a type of traffic that, when sent over a network, is tolerant of delays and changes in the amount of bandwidth it is allocated (e.g., data applications).

**VC (Virtual Channel (or Circuit))** - a communications path between two nodes identified by label rather than fixed physical path.

**VCC (Virtual Channel Connection)** - a unidirectional concatenation of VCLs that extends between the points where the ATM service users access the ATM Layer. The points at which the ATM cell payload is passed to, or received from, the users of the ATM Layer (i.e., a higher layer or ATMM-entity) for processing signify the endpoints of a VCC.

**VCI (Virtual Channel Identifier)** - the address or label of a VC; a value stored in a field in the ATM cell header that identifies an individual virtual channel to which the cell belongs. VCI values may be different for each data link hop of an ATM virtual connection.

**VCL (Virtual Channel Link)** - a means of unidirectional transport of ATM cells between the point where a VCI value is assigned and the point where that value is translated or removed.

**VINES (Virtual Network Software)** - Banyan's network operating system based on UNIX and its protocols.

**Virtual Channel Switch** - a network element that connects VCLs. It terminates VPCs and translates VCI values. The Virtual Channel Switch is directed by Control Plane functions and relays the cells of a VC.

**Virtual Connection** - an endpoint-to-endpoint connection in an ATM network. A virtual connection can be either a virtual path or a virtual channel.

**Virtual Path Switch** - a network element that connects VPLs, it translates VPI (not VCI) values and is directed by Control Plane functions. The Virtual Path Switch relays the cells of a Virtual Path.

**VPT (Virtual Path Terminator)** - a system that unbundles the VCs of a VP for independent processing of each VC.

**VP (Virtual Path)** - a unidirectional logical association or bundle of VCs.

**VPC (Virtual Path Connection)** - a concatenation of VPLs between virtual path terminators (VPTs). VPCs are unidirectional.

**VPDN (Virtual Private Data Network)** - a private data communications network built on public switching and transport facilities rather than dedicated leased facilities such as T1s.

**VPI (Virtual Path Identifier)** - the address or label of a particular VP; a value stored in a field in the ATM cell header that identifies an individual virtual path to which the cell belongs. A virtual path may comprise multiple virtual channels.

**VPL (Virtual Path Link)** - a means of unidirectional transport of ATM cells between the point where a VPI value is assigned and the point where that value is translated or removed.

**VPN (Virtual Private Network)** - a private voice communications network built on public switching and transport facilities rather than dedicated leased facilities such as T1s.

**VT (Virtual Tributary)** - a structure used to carry payloads such as DS1s that run at significantly lower rates than STS-1s.

**WAN (Wide-Area Network)** - a network that covers a large geographic area.

**Warm Start Trap** - a *CellPath* 300 SNMP trap that indicates that SNMP alarm messages or agents have been enabled.

**Yellow Alarm** - an alarm that occurs on a device when the signal from the device is not received at the far-end.

**X.21** - ITU-T standard for serial communications over synchronous digital lines. The X.21 protocol is used primarily in Europe and Japan.

**X.25** - ITU-T standard that defines how connections between DTE and DCE are maintained for remote terminal access and computer communications in PDNs. X.25 specifies LAPB, a data link protocol, and PLP, a network layer protocol. Frame Relay has, to some degree, superseded X.25. See also Frame Relay, LAPB, and PLP.

# Index

**R**

**S**